

UNITED STATES DISTRICT COURT

for the
Western District of Washington



In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with thirteen (13) accounts and
three (3) digital devices, more fully described in
Attachments A-1 and A-2

Case No. MJ22-480

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Information associated with thirteen (13) accounts and three (3) digital devices, more fully described in Attachments A-1 and A-2 and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachments B-1 and B-2, which are attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(e) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

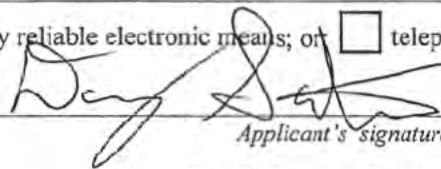
Code Section	Offense Description
18 U.S.C. § 371, 1080A, 1029 1030, 1343, 1349, 1952	Conspiracy, Aggravated Identity Theft, Access Device Fraud, Unauthorized Access to Protected Computer, Wire Fraud, Interstate Travel to Promote Unlawful Activity

The application is based on these facts:

- ☒ See Affidavit of Special Agent Donald Santiso, continued on the attached sheets.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

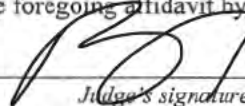
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or ☐ telephonically recorded.


Applicant's signature

Donald Santiso, Special Agent
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 10/05/2022


Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, United States Magistrate Judge
Printed name and title

AFFIDAVIT OF SPECIAL AGENT DONALD SANTISO

STATE OF WASHINGTON)

) ss

COUNTY OF KING)

I, Donald Santiso, being duly sworn under oath, depose and say:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), currently assigned to the Seattle Field Office, and have been so employed since 2019. I am assigned to the Cyber squad where I primarily investigate computer intrusions and other cases involving cybercrimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, Cybercrimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures.

2. I hold Bachelor of Science degree in Computer Engineering. My experience during undergrad included programming in various languages such as Java and C++, circuit analysis, and becoming familiar with computer design and operation. I also hold a certification in cyber security. Prior to my employment as a Special Agent, I worked as a software/test engineer for approximately five years. As part of that employment, I developed programs and engineered tests to assess the capacity of complex computer systems and networks.

PURPOSE OF AFFIDAVIT

3. I submit this affidavit in support of an application under Federal Rule of Criminal Procedure 41 and Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) for a search warrant for data and information associated with the following accounts as further set forth in Attachment A-1:

a. The account admin[REDACTED] (“SUBJECT ACCOUNT 80”), which was stored at premises controlled by Zoho Corporation

1 (“Zoho”) headquartered in Pleasanton, California, and which is currently stored at the
2 FBI Office in Seattle, Washington;¹

3 b. The accounts [REDACTED] (“SUBJECT
4 ACCOUNT 81”), [REDACTED] (“SUBJECT ACCOUNT 82”),
5 [REDACTED] (“SUBJECT ACCOUNT 84”), [REDACTED]
6 (“SUBJECT ACCOUNT 85”), [REDACTED] (“SUBJECT ACCOUNT
7 86”), [REDACTED] (“SUBJECT ACCOUNT 87”),
8 [REDACTED] (“SUBJECT ACCOUNT 88”), and
9 [REDACTED] (“SUBJECT ACCOUNT 89”) which were stored at
10 premises controlled by Google LLC (“Google”) headquartered in Mountain View,
11 California, and which are currently stored at the FBI Office in Seattle, Washington;

12 c. The account [REDACTED] (“SUBJECT
13 ACCOUNT 83”), which was stored at premises controlled by Microsoft Corporation
14 (“Microsoft”) headquartered in Redmond, Washington, and which is currently stored
15 at the FBI Office in Seattle, Washington.

16 d. The Apple iCloud account registered to
17 nishadkunju[REDACTED]@icloud.com (“SUBJECT ACCOUNT 43”), which was stored at
18 premises controlled by Apple, Inc. (“Apple”) headquartered at One Apple Park Way,
19 Cupertino, California, and which is currently stored at the FBI Office in Seattle,
20 Washington.

21 e. The Facebook account bearing digital sign identifier
22 [REDACTED] (“SUBJECT ACCOUNT 51”), which was stored at premises
23 controlled by Meta Platforms, Inc. (“Meta”) headquartered at 1601 Willow Road,
24 Menlo Park, California, and which is currently stored at the FBI Office in Seattle,
25 Washington.

26 f. The account [REDACTED] (“SUBJECT ACCOUNT
27

28 ¹ I have placed brackets around the @ symbols in the email addresses discussed herein, to ensure that those email addresses are not inadvertently hyperlinked in any electronic version of this document.

90”), which was stored at premises controlled by 1&1 Mail & Media, Inc. (“1&1 Mail”) located at 701 Lee Road, Suite 300, Chesterbrook, Pennsylvania, and which is currently stored at the FBI Office in Seattle, Washington.

4. SUBJECT ACCOUNTS 43, 51, and 80 through 90 are collectively referred to herein as the “SUBJECT ACCOUNTS.” Zoho, Google, Microsoft, Apple, Meta, and 1&1 Mail are collectively referred to herein as the “Providers.”

5. This is the second application for search warrants for the SUBJECT ACCOUNTS. On or about October 19, 2020, the Honorable Brian A. Tsuchida, Magistrate Judge for the Western District of Washington, issued warrants to search SUBJECT ACCOUNTS 80-90. On or about May 26, 2020, the Honorable Mary Alice Theiler, Magistrate Judge for the Western District of Washington, issued a warrant to search SUBJECT ACCOUNT 43. On or about August 27, 2020, the Honorable Mary Alice Theiler, Magistrate Judge for the Western District of Washington, issued a warrant to search SUBJECT ACCOUNT 51. The warrants were served on the Providers, and the Providers produced materials to the FBI. By early 2021, the FBI had reviewed the data produced by the Providers, and pursuant to Attachment B of the respective warrants, the FBI identified materials to be seized. The FBI delivered to the United States Attorney’s Office for the Western District of Washington data identifying materials responsive to the warrants, but that data can no longer be found. The FBI still retains the data produced by the Providers, and I am requesting a warrant to search the data related to the SUBJECT ACCOUNTS that is already in the FBI’s custody. This affidavit and application do not request a warrant requiring the Providers to produce additional information related to the SUBJECT ACCOUNTS.

6. I also submit this affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a search warrant for information associated with the following devices (“SUBJECT DEVICES”), which were seized from [REDACTED]

[REDACTED] India:

a. FBI Evidence item 1B110 - 128 GB SanDisk Thumb Drive,

1 b. FBI Evidence item 1B111 - 1 TB WD Hard Drive, and

2 c. FBI Evidence item 1B112 - Black iPhone 8 Plus.

3 7. As described further below, Indian authorities seized the SUBJECT DEVICES
4 and provided them to United States investigators. The SUBJECT DEVICES are currently
5 stored at the FBI Offices in Seattle, Washington, and are further described in Attachment A-
6 2.

7 8. The information to be searched is described in this affidavit and in Attachment
8 A-1 and A-2. The information to be seized is described in more detail in Attachments B-1
9 and B-2. The requested warrants seek authorization to review electronic storage media,
10 electronically stored information, communications, and other records and information to
11 locate evidence, fruits, and instrumentalities described in this affidavit and the
12 attachments. We seek authorization to have any government personnel assisting in the
13 investigation conduct the review of this electronic data for materials responsive to the
14 warrants, such personnel may include, in addition to law enforcement officers and agents,
15 attorneys for the government, attorney support staff, and technical experts. Pursuant to these
16 warrants, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic
17 data to the custody and control of attorneys for the government and their support staff for
18 their independent review.

19 9. Based on my training and experience and the facts as set forth in this Affidavit,
20 there is probable cause to believe that evidence, instrumentalities, contraband, and/or fruits
21 of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1028A (Aggravated
22 Identity Theft), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected
23 Computer), 1343 (Wire Fraud), 1349 (Conspiracy to Commit Wire Fraud), and 1952 (Travel
24 Act) will be found in the SUBJECT ACCOUNTS and SUBJECT DEVICES. In addition,
25 and as discussed below, there is probable cause to believe that the SUBJECT ACCOUNTS
26 and SUBJECT DEVICES were used in furtherance of the criminal scheme under
27 investigation.
28

10. The facts set forth in this affidavit are based upon my personal observations, my training and experience and that of other experienced investigators, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

JURISDICTION

11. Under Federal Rule of Criminal Procedure 41, this Court has venue to issue the requested warrant because the SUBJECT ACCOUNTS and SUBJECT DEVICES, as described in more detail in Attachments A-1 and A-2, are located in the Western District of Washington. In addition, under 18 U.S.C. § 2711, this Court is “a court of competent jurisdiction” because the Court is “a district court of the United States (including a magistrate judge of such a court) . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

STATEMENT OF PROBABLE CAUSE

A. Relevant Background

12. Amazon.com, Inc. (hereinafter, “Amazon”) is a multinational technology company headquartered in Seattle, Washington, within the Western District of Washington. Amazon’s business includes electronic commerce (“e-commerce”), cloud computing, digital streaming, and consumer electronic devices. Amazon operates one of the world’s largest online marketplace platforms, which is commonly referred to as “Amazon Marketplace.” Amazon permits other sellers (referred to as “third-party” or “3P” sellers) to sell products on the Amazon Marketplace. Amazon assigns merchant identification codes comprised of a series of numbers and letters to 3P Seller accounts, and products sold on the Amazon Marketplace are designated by an Amazon Standard Identification Number (or “ASIN”). Amazon takes numerous steps to regulate its marketplace, including through terms of

1 service, restrictions on the sale of counterfeit goods, and enforcement efforts that may result
2 in the suspension of 3P accounts or product listings.

3 13. Amazon provides a number service options to 3P Sellers. One service relevant
4 to this investigation is what is referred to as Fulfillment by Amazon (FBA). FBA is a service
5 by which Amazon stores 3P Sellers goods and provides other services to 3P Sellers,
6 including shipping goods to a 3P Sellers' customers. A part of the FBA program relevant to
7 this investigation is what is referred to as "hazmat" or "hazardous material" storage. At times
8 relevant to this investigation, Amazon designated some goods as "hazardous material" and
9 allowed only certain 3P Sellers to store such material at Amazon facilities for processing
10 through FBA.

11 14. Amazon has a number of rules governing use of the Amazon Marketplace. If a
12 3P Seller violates those rules, Amazon can take enforcement actions against the infringing
13 seller account. Such actions might include suspending the account, which in many cases
14 prevents a 3P Seller from continuing to sell goods on the Amazon Marketplace. 3P Sellers
15 can appeal enforcement actions. Those appeals often take the form of what is referred to as a
16 Plan of Action or POA, which is a written submission by the 3P Seller to Amazon often
17 explaining the reason for the violation, what has been done to fix it, and how the 3P Seller
18 will prevent similar problems in the future. In response to a POA, Amazon decides whether
19 to reinstate the account, continue the suspension, or take other actions.

20 15. To operate the Amazon Marketplace, Amazon uses a number of standard
21 operating procedures, technological tools, algorithms, and other processes, and Amazon
22 keeps much or all of this information confidential. Such confidential information includes
23 standard operating procedures (SOPs), policies, and what are referred to as Wikis and
24 Annotations. Amazon Wikis are knowledge documents strictly for Amazon employees that
25 describe new software tools, procedures, and more. Annotations are Amazon's internal notes
26 regarding enforcement efforts taken against 3P sellers. Amazon takes various steps to keep
27 this information confidential, and based on my review of the evidence in this case, I believe
28 that if a non-Amazon employee possesses such confidential information, there is strong

1 reason to believe the information was acquired through unauthorized access to computer
2 systems, fraud, bribery, or other illicit means.

3 16. Subjects of this investigation used such illicit means to gain access to
4 Amazon's systems controlling the Marketplace and to steal confidential information. This
5 access and information helped individuals on the Amazon Marketplace in many ways,
6 including by reinstating suspended accounts, receiving approval to sell goods usually
7 restricted to certain sellers, winning approval to receive certain services from Amazon, and
8 to gain other competitive advantages over other 3P Sellers.

9 17. The Seattle field office of the Federal Bureau of Investigation (FBI) has been
10 investigating fraud and bribery schemes targeting the Amazon Marketplace. The conduct
11 under investigation includes the payment of commercial bribes to Amazon employees in
12 order to gain unauthorized access to Amazon's computer network, obtain beneficial
13 outcomes for 3P accounts and product listings, take harmful action against competitor 3P
14 accounts and product listings, overcome barriers to the sale of restricted items (e.g.,
15 hazardous items and regulated substances), and misappropriate internal Amazon data.²

16 18. Amazon alerted to the misconduct in or around August and September 2018,
17 when certain Amazon employees located in India admitted, as part of an Amazon internal
18 investigation, that they had accepted bribes from representatives of 3P Seller accounts. The
19 employees admitted that they received payments from these representatives and took steps to
20 benefit their 3P accounts. Financial records, online chat transcripts, and emails, corroborate
21 the payment of the bribes to the employees, as well as the employees' corresponding
22 agreement to confer improper advantages to 3P Sellers by misusing their access to Amazon's
23 computer network.

24 19. In or around the end of August and September 2018, Amazon terminated the
25 employees who admitted to participating in the scheme. As confirmed through this
26
27

28 ² The government has obtained warrants over the course of this investigation in various federal judicial districts. This affidavit does not cover all of the facts set forth in those earlier affidavits, but instead sets out only the facts relevant to the determination of probable cause as to the SUBJECT ACCOUNTS and SUBJECT DEVICES.

1 investigation, including the review of communications and financial records, the terminated
2 Amazon employees included Nishad Kunju (“Kunju”), E.E., and R.B. The review of
3 documents, financial records, and communications showed that these three individuals
4 continued to participate in the scheme even after they were fired. They used their knowledge
5 of the Amazon Marketplace and Amazon’s organization structure, as well as their contacts
6 within Amazon to help others continue their bribery and fraud schemes. For instance,
7 following the termination of employment from Amazon, Kunju recruited existing Amazon
8 employees to provide Amazon information and access to Amazon’s systems in exchange for
9 payments, and managed their work and compensation for projects assigned by others.

10 20. In the course of the investigation, the FBI identified some of the entities and
11 individuals based in the United States who worked together to bribe Amazon employees.
12 Those entities and individuals included Digital Checkmate, Inc. (“Digital Checkmate”),
13 Digital Checkmate’s executives Joseph Nilsen (“Nilsen”) and Kristen Leccese (“Leccese”),
14 Ephraim Rosenberg (“Rosenberg”), Hadis Nuhanovic (“Nuhanovic”), and Rohit Kadimisetty
15 (“Kadimisetty”).

16 21. On September 16, 2020, a Grand Jury in the Western District of Washington
17 returned an Indictment charging six individuals with crimes relating to the conduct under
18 investigation, specifically, with (a) conspiring to commit violations of the Travel Act
19 (specifically through commercial bribery), and to access a protected computer without
20 authorization, in violation of 18 U.S.C. § 371; (b) conspiring to commit wire fraud, in
21 violation of 18 U.S.C. § 1349; and (c) committing wire fraud, in violation of 18 U.S.C.
22 § 1343. *See United States v. Rosenberg, et al.*, CR20-151RAJ, Dkt. 1. The six individuals
23 charged in the Indictment were Ephraim Rosenberg, Joseph Nilsen, Hadis Nuhanovic,
24 Kristen Leccese, Rohit Kadimisetty, and Nishad Kunju. Five of the six defendants have
25 appeared in the charged case. (Nishad Kunju is the only defendant who has not appeared in
26 the case, and investigators believe he still lives in India.) Of the five defendants who have
27 appeared, four have pleaded guilty to at least one of the charged crimes. Ephraim Rosenberg
28

1 is the only defendant who has yet to plead guilty before trial, which is scheduled to begin in
2 February 2023.

3 **B. Previous Legal Process for Rosenberg Email Account**

4 22. On or about August 27, 2020, the Honorable Mary Alice Theiler issued a
5 warrant to search the email account reinstatement911[*@*]mail.com. As explained in the
6 affidavit in support of the application for that search warrant, Ephraim (“Ed”) Rosenberg
7 used reinstatement911[*@*]mail.com to exchange emails with an email address
8 ([REDACTED]), with which Rosenberg also exchanged emails from another
9 email address (reinstatement911[*@*]gmail.com).³ The prior affidavit also explained that
10 there was probable cause to believe that Rosenberg used reinstatement911[*@*]mail.com to
11 solicit work that required the payment of commercial bribes to Amazon insiders.

12 23. Registration records from 1&1, the company that provides the account
13 reinstatement911[*@*]mail.com, establish that the account is Rosenberg’s account.
14 Specifically, those registration records show that the account is registered under the name
15 “Ephraim Rosenberg” and a street address which aligns with Rosenberg’s known residence
16 in Brooklyn, New York.⁴ The registration records also show that Rosenberg listed his other
17 known email address (reinstatement911[*@*]gmail.com) as the alternative email account for
18 the reinstatement911[*@*]mail.com address. Finally, those records show logins from at least
19 one Internet Protocol (“IP”) address that Rosenberg used to log into various PayPal accounts
20 registered under his own name, bank accounts, and email addresses, as well as other
21 electronic accounts in his name. When registering the account, Rosenberg appeared to
22 provide a date of birth that is not his actual date of birth.

23 24. Records found in reinstatement911[*@*]mail.com pursuant to the above-
24 mentioned warrant establish that Rosenberg used that account to communicate with several
25

26 ³ There were two different accounts with the same prefix “reinstatement911.” The difference was in the suffix, which
27 was “*@*mail.com” for one account and “*@*gmail.com” for the other. This difference reflects that the account ending
28 “*@*mail.com” was registered with a company called 1&1 Mail & Media, Inc., and the account ending “*@*gmail.com”
was registered with Google.

⁴ On or about August 16, 2020, law-enforcement agents searched Rosenberg’s residence in Brooklyn, NY, pursuant to a
warrant issued by the U.S. District Court for the Eastern District of New York.

people regarding the performance of work that required the use of apparently corrupted Amazon employees and contractors. The people with whom Rosenberg communicated include the users of some of the SUBJECT ACCOUNTS. More specifically:

SUBJECT ACCOUNTS 80-83

- [REDACTED] (“SUBJECT ACCOUNT 80”)
- [REDACTED] (“SUBJECT ACCOUNT 81”)
- [REDACTED] (“SUBJECT ACCOUNT 82”)
- [REDACTED] (“SUBJECT ACCOUNT 83”)

25. Rosenberg used reinstatement911[REDACTED]@mail.com to communicate with [REDACTED] (i.e., SUBJECT ACCOUNT 80). Specifically, investigators found more than 60 emails between reinstatement911[REDACTED]@mail.com and SUBJECT ACCOUNT 80 in the “Drafts” folder of the reinstatement911[REDACTED]@mail.com account. In my training and experience, there is probable cause to believe that storing emails to the “Drafts” folder in this manner enabled Rosenberg to carry on some of his email communications without actually transmitting emails (i.e., by permitting different users to log into the account, make changes to draft unsent emails and thereby communicate with one another without creating an electronic transmission that could be traced by law enforcement). In any case, however, some of the emails with SUBJECT ACCOUNT 80 found in the “Drafts” folder reflect emails that *were* transmitted between reinstatement911[REDACTED]@mail.com and SUBJECT ACCOUNT 80 regarding services that appeared to require the use of Amazon insiders. In those emails, the user of SUBJECT ACCOUNT 80 used the pseudonym “Mark Stevens.”

26. For instance, between on or about June 11, 2018 and on or about June 15, 2018, Rosenberg exchanged emails with SUBJECT ACCOUNT 80 regarding the retrieval of “notes” from an Amazon insider, as well as potential increases to a third-party seller account’s hazmat storage allowance in Amazon’s warehouses. The text of that email exchange is as follows:

1 **ROSENBERG:** “today?”⁵

2 **SUBJECT ACCOUNT 80:** “I am waiting to get it, they keep saying with Amazon
3 changes it has slowed down the process to get the notes, they are working on it.”

4 **ROSENBERG:** “ok – hazmat can do?”

5 **SUBJECT ACCOUNT 80:** “Yes, but the storage amount is very limited now, from
6 200 units to 1k they can build more storage if they have good sales amazon will start
7 increasing the amount.”

8 **ROSENBERG:** “cost?”

9 **SUBJECT ACCOUNT 80:** “Price is \$2000 what is worth is getting in the program
10 which is less than 1% of people who makes it now. Also wanted to let you know that
11 my contact wants to get paid more for this notes as it is to grossly undervalued for the
12 amount you are sending and the cost we sell per note to other people. We can do now
13 \$600 a week as my contact also has a hard time pulling the information as Amazon
14 system is very slow these past weeks because of updates they are doing. We are sure
15 this is still a fair price to you as we are sure this is a very profitable area.

16 **ROSENBERG:** “thats a big jump – can we do 500?”

17 **SUBJECT ACCOUNT 80:** “Yes, I understand is a big jump but yes \$500 is
18 something we can agree is our partners that requests this type of things but we can
19 work on that.”

20 **ROSENBERG:** “ok ty”

21 **SUBJECT ACCOUNT 80:** “You are welcome.”

22 27. In my review of other records in this case, including emails that Rosenberg
23 exchanged with Joseph Nilsen (“Nilsen”), another defendant charged in the Indictment and
24 one who pleaded guilty to conspiracy to commit wire fraud and conspiracy to violate the
25 travel act through commercial bribery, I have probable cause to believe that the term “notes”
26 refers to annotation histories regarding third-party accounts. These annotation histories often
27
28

⁵ Rosenberg’s first email in the chain used the subject line “today?” but did not contain any other content.

1 included Amazon's internal notes explaining how an account had infringed Amazon's rules,
 2 what steps Amazon had taken with regard to that account, and why it had taken them. Based
 3 on my review of records in this case, I know that Amazon maintained these "notes" on its
 4 protected computer network, and Rosenberg regularly asked Nilsen to misappropriate them
 5 (i.e., through the use of corrupted Amazon employees and contractors) in order to obtain
 6 information about internal processes with respect to those accounts.⁶ Rosenberg also used
 7 the term "hazmat" in emails with Nilsen, in order to refer to increases in hazmat storage,
 8 which corrupted Amazon employees and contractors accomplished by using their access
 9 credentials to artificially zero out Amazon's calculation of third-party sellers' hazmat
 10 storage, in order to induce Amazon's internal systems into concluding in error that those
 11 sellers had not used any storage.

12 28. In addition to the email exchange, investigators also found a March 2019 email
 13 exchange between reinstatement911[.]mail.com and SUBJECT ACCOUNT 80 about the
 14 reinstatement of third-party seller accounts that Amazon had suspended.

15 29. The subject line of Rosenberg's original email in the email string was "eta?"
 16 Following that email, the two users engaged in the following exchange:

17 **SUBJECT ACCOUNT 80:** "Notes will be coming soon, but, I will get in touch with
 18 you soon as things are not working out for us."

19 **ROSENBERG:** "meaning?"

20 **SUBJECT ACCOUNT 80:** "We will connect with you in the afternoon and discuss
 21 it."

22 **ROSENBERG:** "but todays will get before right?"

23 **SUBJECT ACCOUNT 80:** "Yes, we will send them"

24 **ROSENBERG:** "do you have them?"

25 **SUBJECT ACCOUNT 80:** "We sent them on this email. We were going to discuss
 26 that account notes are way undervalued. People is realizing of the value they get for
 27

28 ⁶ In his email exchanges with Nilsen, Rosenberg used the term "fruit" to refer to misappropriated annotation records from Amazon's internal computer network.

1 reinstating accounts. We can't keep this super low prices anymore we did it as
2 introduction until people understand the value. We sell at \$100 per note and last
3 month you requested over 120 notes. We can give you still a good price as we are
4 certain you guys are making 10s of thousands of dollars per month on suspensions
5 along, lets try to stop the greed and lets start sharing we can do \$8000 a month for the
6 notes, we know you can do it but you have to start looking me as a partner not
7 someone who sells cheap and get advantage from this.”

8 **ROSENBERG:** “hi – thats way to *[sic]* big of a jump –”

9 **SUBJECT ACCOUNT 80:** “Yes, it is a big bump from where we are but you know
10 is a fair price. Because I know the suspension business and consulting business,
11 ASINs blocks, metrics check it generates a lot of revenue and I know it and you know
12 and I am sure your revenue is in the tens of thousands of \$. I am not asking a lot from
13 what you are getting from this business, just saying lets not to be greedy none of us, I
14 am not asking the full amount the notes you are getting are worth and you are giving a
15 fair share of what I am sending as it has a lot of value. I know the advantage the notes
16 give for appeals and which cases to take and not to take, it saves a lot of time and
17 money, every agent has its own way of thinking and each case is different that is why
18 notes give that extra edge needed to succeed but it takes time to perfection the method
19 which at this point I am sure you guys also did.”

20 **ROSENBERG:** ““stop the greed” – I sent what we agreed’

21 **SUBJECT ACCOUNT 80:** “Yes, I know what you said. I said lets not be greedy
22 none of us and come to an agreement where we both get a fair share and not take
23 advantage from you or you from me. We need a new agreement where both of us can
24 make money as what I am getting from the notes is far more than what I am receiving
25 from our agreement.”

26 **SUBJECT ACCOUNT 80:** “We need to know if you want to keep going with the
27 supply, we need to price correctly this service as you know is worth what we are
28

1 asking. It has been way to long we have been working together now, but let me know
2 as we need to know our next steps.”

3 **ROSENBERG:** “either way lets finish the week – I can go up a bit by not so
4 dramatic – maybe we can do 50 each one?”

5 **SUBJECT ACCOUNT 80:** “We can do \$65 each at a minimum request of 30 per
6 week or we can do \$60 if you keep the current amount of requests which is over 120.
7 We have to price the service properly as you know it is undervalued and you are
8 making a nice profit so, we need to make our cut as well and I am sure you
9 understand.”

10 **ROSENBERG:** “lets just keep it like it was 650 a week”

11 **SUBJECT ACCOUNT 80:** “You have to understand we need to make it worth it to
12 keep going or we will perform the other plans we have for the notes... \$1750 a week”

13 **ROSENBERG:** “no way – way way too much – will move to 800”

14 **SUBJECT ACCOUNT 80:** “I am sure you are doing big money with suspensions, we
15 need to negotiate \$800 is just not going to work for us, lets do \$1550, math does not
16 lie you are still clearing a lot of money for you.”

17 **ROSENBERG:** “let me know if 900 can work please”

18 **SUBJECT ACCOUNT 80:** “Lets talk about it tomorrow”

19 **ROSENBERG:** “please lets finish this week either way as agreed”

20 **SBUEJCT ACCOUNT 80:** “Ok, lets finish this week, send me requests up to more
21 30 more only”

22 30. Dozens of other emails found in the reinstatement911[[@](#)]mail.com “Drafts”
23 folder reflected that messages had been exchanged between Rosenberg and the user of
24 SUBJECT ACCOUNT 80 on various dates, but the emails were either blank or contained
25 only a subject line. One example of such an email is below:
26
27
28

[No Subject]

From: John Smith <reinstatement911@mail.com>
 To: [REDACTED]
 Date: Mon, 03 Sep 2018 19:37:44 -0700

31. Another example, with a subject line showing a merchant identification number (a number that identifies a specific 3P Seller account) that appears to correspond to a third-party account operating on the Amazon Marketplace, is shown below:

[REDACTED]

From: John Smith <reinstatement911@mail.com>
 To: [REDACTED]
 Date: Wed, 27 Mar 2019 14:38:44 -0700

32. In my training and experience, emails with no content whatsoever could reflect the conduct generally described above, i.e., Rosenberg's use of the "Drafts" folder of his email account to communicate with others, without actually transmitting any emails. With respect to the emails that contained only a merchant identification number in the subject line, I am aware based on my review of other emails exchanged between Rosenberg and Nilsen that Rosenberg regularly used shorthand to communicate with the individuals to whom he sent work. Specifically, in numerous emails to Nilsen, Rosenberg included a merchant identification number in the subject line, in order to convey to Nilsen that he needed annotation records misappropriated from Amazon's computer network with regard to that third-party seller account.

33. Records produced by PayPal establish probable cause to believe that, as reflected by the emails set out above, Rosenberg paid the user of SUBJECT ACCOUNT 80 for the services described in the emails. Specifically, PayPal produced records showing that Rosenberg registered a PayPal account under the email address reinstatement911[]mail.com (the “reinstatement911 PayPal account”). When registering the reinstatement911 PayPal account, Rosenberg provided the name “Tom Landry.”⁷ Rosenberg also provided PayPal with two bank account numbers for accounts at HSBC Bank USA, N.A. and JPMorgan Chase, both of which are registered to a New York business named Effyzaz, Inc. (“Effyzaz”), which Rosenberg owns. Other records in the reinstatement911 PayPal account also show that it is Rosenberg’s, including the fact that the account received over twenty thousand dollars in transfers from another PayPal account registered under Rosenberg’s email address effyrosenberg[]gmail.com, which Rosenberg uses in connection with his legitimate business. The fact that a PayPal account registered under effyrosenberg[]gmail.com financed the reinstatement911 PayPal account establishes probable cause to believe that Rosenberg transferred funds into the latter account so that he could make payments for the services described above.

34. Transaction records for the reinstatement911 PayPal account show that, between in or about December 2017 and on or about August 16, 2020, the reinstatement911 PayPal account made transfers to four email addresses associated with a PayPal account registered under the name “[REDACTED],” including SUBJECT ACCOUNT 80, as well as SUBJECT ACCOUNTS 81 through 83.⁸

35. Those transfers are shown in the chart below.

⁷ Tom Landry was a professional football player and then a head coach for the NFL team the Dallas Cowboys. According to public sources, Landry died in February 2000.

⁸ Records produced by PayPal show that Subject Accounts 80 through 83 were among several email addresses associated with a PayPal account registered under the name “[REDACTED].” The other email addresses associated with that PayPal account were “[REDACTED],” “[REDACTED],” and “[REDACTED].”

Recipient Email Address	Amount Transferred (before PayPal fees)	Number of Transfers
SUBJECT ACCOUNT 80	\$18,420 ⁹	37
SUBJECT ACCOUNT 82	\$50,100	33
SUBJECT ACCOUNT 81	\$46,050	38
SUBJECT ACCOUNT 83	\$0 ¹⁰	0
Total	\$114,570	108

36. In addition to using the reinstatement911 PayPal account to make transfers to the PayPal account registered under SUBJECT ACCOUNT 80, Rosenberg also used a different PayPal account registered under the email address effyrosenberg[@]gmail.com to make such transfers. Records found in the investigation show that effyrosenberg[@]gmail.com is Rosenberg's official email address, which he uses in connection with his consulting business. The PayPal account registered under effyrosenberg[@]gmail.com was registered under Rosenberg's true name, his actual residence, and bank account registered to his company, Effyzaz, Inc. Through that account, Rosenberg transferred \$17,188 to a PayPal account registered to SUBJECT ACCOUNT 80 between on or about January 13, 2017, and on or about March 6, 2018.

37. In my training and experience, including through my review of records in this case, I am aware that, when a transfer is attempted to be made to/from an email address associated with a PayPal account, PayPal sends an email to the email addresses that participated in the transaction. Thus, in this case, there is probable cause to believe that SUBJECT ACCOUNTS 80 through 83 received confirmation emails about the PayPal transfers sent by Rosenberg, whether those transfers were attempted or completed. There is

⁹ PayPal records show that the reinstatement911 PayPal account made an additional \$1,700 transfer to a PayPal account registered under SUBJECT ACCOUNT 80, but that transfer was "refunded," which appears to indicate the recipient PayPal account sent the funds back after receiving them.

¹⁰ PayPal records show that the reinstatement911 PayPal account made four transfers to a PayPal account registered under SUBJECT ACCOUNT 83. The transfers collectively were worth \$3,200, and each transfer occurred on a different date. However, all four of the transfers were "refunded," which appears to indicate that the recipient PayPal account sent the funds back.

1 also probable cause to believe that information in the accounts will help to identify the
2 user(s) of the accounts.¹¹

3 38. On or about December 17, 2020, the government conducted a virtual proffer
4 interview with Rosenberg. During the interview, Rosenberg was asked clarifying questions
5 regarding some of the SUBJECT ACCOUNTS. Rosenberg explained that in 2017 he reached
6 out to [REDACTED] looking for annotations. As explained above, I believe that
7 “annotations” or “notes” are internal Amazon records regarding 3P Seller accounts that
8 operate on the Amazon Marketplace. According to Rosenberg, [REDACTED] worked for [REDACTED]
9 [REDACTED] and lived in Costa Rica. Rosenberg further explained that [REDACTED] used several
10 different email addresses to communicate with Rosenberg, including SUBJECT ACCOUNT
11 80 and SUBJECT ACCOUNT 82. According to Rosenberg, [REDACTED] would provide the
12 annotations using Google Docs instead of email as he felt that was safer and Rosenberg paid
13 [REDACTED] via multiple PayPal accounts operated by [REDACTED] using different names such as
14 “[REDACTED]”, “[REDACTED]” (same name as SUBJECT ACCOUNT 83), and
15 “[REDACTED]”.

17 SUBJECT ACCOUNT 84

- 18 • [REDACTED] (“SUBJECT ACCOUNT 84”)

19 39. There is also probable cause to believe that the email account
20 [REDACTED] (i.e., SUBJECT ACCOUNT 84) will contain evidence of the
21 crimes under investigation. Records found in the reinstatement911[REDACTED]@mail.com account
22 show that Rosenberg used that account to communicate with SUBJECT ACCOUNT 84
23 about the same type of work about which Rosenberg communicated with others, such as
24 Nilsen and SUBJECT ACCOUNT 80. In those emails, the user of SUBJECT ACCOUNT
25

26
27 ¹¹ Although the transaction records for the reinstatement911 PayPal account distinguish transfers between the different
28 email addresses to which Rosenberg sent money, the transaction records for the recipient PayPal account show all of the
transfers as having been “received by” the email address [REDACTED] (SUBJECT ACCOUNT 81). In
my training and experience, I believe that may be because PayPal allows an accountholder to designate several recipient
email addresses, but to have any payments sent to those email addresses routed to the same common destination.

1 84 used the name "[REDACTED]" ("[REDACTED]") to identify himself. Publicly available records
2 on the social-networking site Facebook reviewed in 2020 showed that a user named
3 "[REDACTED] ([REDACTED])" maintained a profile page, in which he identified
4 himself as a "Sr. Vendor Management Executive" of an Amazon entity in India named
5 "Amazon Development Centre," and in which he claimed that he had held that position in
6 the city of Hyderabad, India since July 26, 2016.

7 40. In a letter dated November 3, 2020, Amazon's attorneys informed investigators
8 that Amazon had employed an individual named [REDACTED], who had been hired in
9 July 2016 and who had worked in Selling Partner Support, a team that provided customer
10 support to sellers. The letter further explained that [REDACTED] was based in Amazon's office
11 in Bangalore, India, and had access to Amazon non-public, confidential data. The letter also
12 stated that on Amazon's internal employee directory, [REDACTED] provided the nickname
13 "[REDACTED]" and that [REDACTED] had left Amazon on December 3, 2018.

14 41. In reviewing emails from Rosenberg's reinstatement911[REDACTED]@mail.com account,
15 investigators found the email exchange below, in which Rosenberg asked [REDACTED] about
16 whether it is "possible to enable" in connection with an apparent merchant identification
17 number contained in the subject line of the email:
18
19
20
21
22
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Re: [REDACTED]

From: John Smith <reinstatement911@mail.com>
To: [REDACTED] <[REDACTED]>
Date: Thu, 06 Dec 2018 07:17:53 -0800

Sent: Thursday, December 06, 2018 at 10:06 AM
From: [REDACTED] <[REDACTED]>
To: "John Smith" <reinstatement911@mail.com>
Subject: Re: [REDACTED]

Reasons :

Vendor account got impacted due to Keyword infringement as per TID:5385186471, 5385293421, 5385245971

PDP Tampering on over 300 ASIN's.

=====

Yes, possible to activate the account but will require \$2000. I will remove these remarks from the account and then activate the account.

On Wed, 5 Dec, 2018, 5:57 PM John Smith <reinstatement911@mail.com> wrote:
possible to enable

42. Investigators also found the email chain below, in which Rosenberg and [REDACTED] discussed whether [REDACTED] could "get the seller performance team annotations" regarding a third-party merchant account, which Rosenberg identified in the subject line of his email. As discussed above, "annotations" are internal Amazon notes regarding 3P Seller accounts that operate on the Amazon Marketplace.

Re: [REDACTED]

From: John Smith <reinstatement911@mail.com>
To: [REDACTED] <[REDACTED]>
Date: Sun, 09 Dec 2018 05:00:34 -0800

Sent: Sunday, December 09, 2018 at 4:00 AM
From: [REDACTED] <[REDACTED]>
To: "John Smith" <reinstatement911@mail.com>
Subject: Re: [REDACTED]

I can get the seller performance team annotations.

Just the basic annotations can only be provided.

On Sun, 9 Dec, 2018, 11:45 AM John Smith <reinstatement911@mail.com> wrote:
if possible (not like last time)

43. In other emails, Rosenberg and [REDACTED] discussed the reinstatement of suspended merchant accounts. In two instances, [REDACTED] initially stated that he believed that he could reinstate a suspended account, and accepted payment from Rosenberg for that inside assistance, but later told Rosenberg that he could not complete the job. In those cases, Rosenberg and/or [REDACTED] discussed [REDACTED] refunding Rosenberg's initial payment. Investigators reviewed PayPal records associated with reinstatement911[REDACTED]@mail.com and identified several payments to "[REDACTED]" partially refunded. In addition to those emails, investigators also found blank emails saved in the "Drafts" folder, indicating that Rosenberg may have used the "Drafts" folder to exchange messages with [REDACTED] without actually transmitting any emails that could be traced by law enforcement.

44. In the letter from Amazon's counsel on November 3, 2020, Amazon's counsel stated that it had not identified any suspicious activity during the relevant time period involving vendor code [REDACTED], [REDACTED], and another identifying number found in other messages between Rosenberg and [REDACTED]. Amazon's counsel, however, did explain that for another vendor code discussed by [REDACTED] and Rosenberg, records did indicate that [REDACTED] accessed and viewed the account on November 29, 2018, without a valid workflow justification. Amazon's counsel also stated that Amazon records implicated [REDACTED] in potentially unlawful conduct after his departure from Amazon because on May 17, 2019, a former Amazon employee admitted to Amazon internal investigators that he had accepted bribes and colluded with [REDACTED] to exfiltrate Amazon data.

45. Records from the reinstatement911 PayPal account show that Rosenberg made transfers to a PayPal account registered under SUBJECT ACCOUNT 84. Specifically, on or about November 29, 2018, Rosenberg transferred \$1,500 to [REDACTED], and on or about December 6, 2018, Rosenberg transferred \$2,200 to [REDACTED]. PayPal records state that both of those transfers were "Partially Refunded."

SUBJECT ACCOUNT 85

- [REDACTED] ("SUBJECT ACCOUNT 85")

46. There is also probable cause to believe that [REDACTED] (i.e., SUBJECT ACCOUNT 85) will contain evidence of the crimes under investigation. Records found in the investigation suggest that [REDACTED] is an email account used by an individual named [REDACTED] (“[REDACTED]”), who is suspected to be operating a service named “Amzn Insider Help,” through which he provides a range of services to third-party sellers on the Amazon Marketplace. Based on my experience with this case, I believe that the kinds of services [REDACTED] offered rely on the payment of commercial bribes to Amazon employees and contractors, in exchange for which those employees and contractors misappropriate information from Amazon’s computer network, misuse their access fraudulently, and otherwise exceed their authorized access to Amazon’s network.¹²

47. Rosenberg used reinstatement911[REDACTED]@mail.com to exchange emails with SUBJECT ACCOUNT 85 regarding work that, I believe, required the use of corrupted insiders. For instance, in the September 11, 2019 email shown below, the user of SUBJECT ACCOUNT 85 sent an email to Rosenberg advertising services that included “Account reinstatement 100% by insider 5000\$,” as well as “[f]eedback removal” and “[r]einstatement any ASIN.” Based on my review of records regarding the Amazon Marketplace, I am aware that “reinstatement” is a term used to refer to the act of reviving a product or account on the Amazon Marketplace that Amazon had suspended for reasons that may include the violation of Amazon’s codes of conduct, product-safety concerns, and/or counterfeiting concerns. I am also aware that the term “[f]eedback” is a term used to refer to product reviews placed by consumers on the Amazon Marketplace.

¹² In or about November 2019, a purported consultant to third-party merchants named [REDACTED] (“[REDACTED]”) approached Amazon’s in-house lawyers and purported to provide documents describing [REDACTED]’s services, and some of the electronic accounts that [REDACTED] used. In the course of its investigation, the government has identified evidence that shows that [REDACTED] paid Nilsen to engage in fraud and commercial bribery in connection with the Amazon Marketplace, and that [REDACTED] himself referred to his access to corrupted Amazon employees and contractors. In part because of [REDACTED]’s status as a subject of the government’s investigation, the government has not relied on any of the material that [REDACTED] produced to Amazon’s legal team when taking investigative steps.

New services

From: [REDACTED]
 To: reinstatement911@mail.com
 Date: Wed, 11 Sep 2019 13:21:43 -0700

Account reinstatement 100% by insider 5000\$
 -need merchant ID
 -account email
 -reason for suspension
 -3-5 days

Feedback removal 100% - 55\$ per 50+ 45\$ per
 -order ID
 -marketplace
 -merchant ids
 -1-2 days

Reinstate any ASIN 100% - 3000\$
 -need ASIN
 -merchant ID
 -main email
 -3-5 days

48. Likewise, in this August 4, 2019 email, the user of SUBJECT ACCOUNT 85 informed Rosenberg that he could “delete intellectual complaints,” which I believe is a reference to intellectual-property complaints made against products sold on the Amazon Marketplace:

[No Subject]

From: [REDACTED]
 To: reinstatement911@mail.com
 Date: Sun, 04 Aug 2019 14:00:42 -0700

Sir I can delete intellectual complaints .
 90% success, if it doesn't work out - I return the full money - it is 650USD

49. The user of SUBJECT ACCOUNT 85 also sent Rosenberg the following August 15, 2019 email, describing how an “Amazon insider [can] unlock your account, directly.”

[No Subject]

From: [REDACTED]
 To: reinstatement911@mail.com
 Date: Thu, 15 Aug 2019 20:42:04 -0700

Hi My friend, Good news! Received a notification: Amazon insider can unlock your account, directly. It means no need to appeal it, the internal help you unblock directly. You need to provide marketplace and Amazon Registry Emails. Then we will give you cost. This price is at least 5,000usd. If you think it's not necessary to save it, don't send it. Besides, we have other Amazon Services or you need our service list, Please feel free tell us, Thank you very much.

50. In another email, the user of SUBJECT ACCOUNT 85 invited Rosenberg to “[j]oin the telegram group for all the updates and new services,” and signed the email “[REDACTED].” In my training and experience, I am aware that Telegram is an encrypted messaging application. I am also aware that intermediaries to corrupted Amazon employees and contractors regularly use encrypted messaging applications to communicate with clients and with corrupted Amazon insiders, in order to protect their communications from potential discovery.

51. In addition to the emails described above, which investigators found in Rosenberg’s email inbox, investigators also found more than 30 emails in the “Drafts” folder of reinstatement911[REDACTED]@mail.com, which appeared to depict deleted conversations between reinstatement911[REDACTED]@mail.com and the user of SUBJECT ACCOUNT 85. Many of those “Draft” emails contained no subject line or other content, which appears to indicate that they had been purged of their original text. However, some emails reflected conversations between Rosenberg and the user of SUBJECT ACCOUNT 85 about the performance of work that required the payment of commercial bribes to corrupted Amazon employees and contractors, such as the email below:

Re: info

From: John Smith <reinstatement911@mail.com>
To: [REDACTED]
Date: Wed, 25 Oct 2017 06:45:27 -0700

Sent: Wednesday, October 25, 2017 at 8:09 AM
 From: [REDACTED]
 To: "John Smith" <reinstatement911@mail.com>
 Subject: Re: info

I have this ready
 send 250\$

On Oct 24, 2017, at 2:39 PM, John Smith <reinstatement911@mail.com> wrote:

[REDACTED]
 please send asap and confirm

52. Records produced by PayPal show that, between in or around August 2017 and in or around October 2017, Rosenberg sent \$10,870 to a PayPal account registered under SUBJECT ACCOUNT 85. Specifically, Rosenberg transferred those funds from a PayPal account registered under the email address effyrosenberg[.]gmail.com, which is an email address that he uses in connection with his consulting business, and in which he identifies himself by his own name. Records produced by PayPal show that a PayPal account registered to [REDACTED] (which is very similar to SUBJECT ACCOUNT 85) received payments from numerous other PayPal users, who the government is continuing to attempt to identify in its ongoing investigation.

53. Based on the facts set out above, I respectfully submit that there is probable cause to believe that SUBJECT ACCOUNT 85 has been used by an individual who offers services that require the use of Amazon "insiders," in exchange for commercial bribes paid to those "insiders." I also believe that Rosenberg was one of the clients of those services. Records found in SUBJECT ACCOUNT 85 may shed light on the details of these services, as well as the identities of other clients like Rosenberg.

SUBJECT ACCOUNTS 86 and 87

- [REDACTED] ("SUBJECT ACCOUNT 86")
- [REDACTED] ("SUBJECT ACCOUNT 87")

54. There is also probable cause to believe that [REDACTED] ("SUBJECT ACCOUNT 86") and [REDACTED] ("SUBJECT ACCOUNT 87") will contain evidence of the crimes under investigation. Records found in reinstatement911[.]mail.com show that Rosenberg exchanged emails with both of these accounts in connection with services that required the payment of commercial bribes to corrupted Amazon employees and contractors. In one of those emails, the user of SUBJECT ACCOUNT 86 used the following signature block, in which he identified himself as a purported "Amazon Ungating Specialist":

Thanks,
[REDACTED] AKA [REDACTED]
[REDACTED] Consultant, Amazon Ungating Specialist
Email: [REDACTED]
Amazon Ungating Service: [www.\[REDACTED\].com](http://www.[REDACTED].com)
FB Group: [www.facebook.com/groups/\[REDACTED\]](http://www.facebook.com/groups/[REDACTED])

55. In my review of other investigative materials in this case, I am aware that the term "ungating" refers to the process by which Amazon grants 3P Sellers approval to sell products in certain restricted product categories, including, e.g., dietary supplements and copyrighted multimedia. The conduct under investigation in this case includes the use of forged and fraudulent material, as well as the payment of commercial bribes to corrupted Amazon employees and contractors, in order to obtain such category approval.

56. In one email chain with Rosenberg, the user of SUBJECT ACCOUNT 86 told Rosenberg to send him the correct "login" identifier for a merchant account with which Rosenberg had sought assistance. After providing the user of SUBJECT ACCOUNT 86 with that login information, Rosenberg asked to "let me know if your [sic] on it – and when

1 | you think will be reinsatted [*sic*].” In response, the user of SUBJECT ACCOUNT 86 stated
2 | that “we need to start from the beginning.”

3 | 57. In another email chain between SUBJECT ACCOUNT 86 and Rosenberg,
4 | Rosenberg used the subject line “reinstatement” and asked “whats the process.” In response,
5 | the two individuals engaged in an exchange in which Rosenberg explained that a third-party
6 | merchant account suspected to be used by one of his clients had been suspended because it
7 | used “forged docs, but only because the real invoices would not have been invoice
8 | guidelines.” In my review of other investigative records, I am aware that Amazon
9 | sometimes requires third-party merchants to submit invoices from a *bona fide* supplier as a
10 | precondition to obtaining category approval, and in order to establish to Amazon that the
11 | products they seek to sell were legitimate and not counterfeit. I am also aware that some
12 | merchants use forged invoices in order to deceive Amazon into believing that they had
13 | purchased products from a *bona fide* supplier prior to seeking category approval.

14 | 58. Later in the email exchange, the user of SUBJECT ACCOUNT 86 told
15 | Rosenberg: “here is the plan[.] total 9k[.] 6k now to get started..3k after reinstatement[.] if
16 | we failed means 120% refund of that \$6K[.] let’s do it? go to www.thefunnelguru.com
17 | choose \$2000 plan and pay thrice.... Don’t fill the form[.] we need 2-4 days but set the
18 | expectation with sellers as less than 7 days[.] let’s do it?” When Rosenberg asked for a
19 | lower price than the price quoted by SUBJECT ACCOUNT 86, the user of SUBJECT
20 | ACCOUNT 86 responded:

21 | Sorry, these are high level connections and we take any case to get activated
22 | regardless of the reasons and number of appeals. I know you have potential clients
23 | and that’s why I said 9K instead of 12k. this is what I can do it.. 6k to start with and
24 | then 1k after reinstatement (total 7k instead of 12k) considering you will be getting us
25 | more clients in future to strengthen our business relationship. Last night one seller
26 | who is making 30k in sales paid us 12k get his account back. to be honest my
27 | commission is nothing in this case as I have to pay lot to others. Let me know happy
28 | to help you.

1 59. After Rosenberg agreed on the price, the two individuals discussed payment.
2 The user of SUBJECT ACCOUNT 86 offered Rosenberg an option between paying via
3 “paypal friends and family” or “via debit/credit card.”

4 60. When Rosenberg responded that he sought to pay by credit card, the user of
5 SUBJECT ACCOUNT 86 instructed Rosenberg to browse to the website
6 www.thefunnelguru.com and to make payment on a payment portal on that website.
7 Rosenberg indicated that he had made the payment and then later stated that he was not
8 “comfortable” and asked for a refund. The user of SUBJECT ACCOUNT 86 stated that the
9 work had already begun on the reinstatement request by the “team” and Rosenberg did not
10 maintain his request for a refund.

11 61. Investigators found other emails between SUBJECT ACCOUNT 86 and
12 Rosenberg. Like the emails with other SUBJECT ACCOUNTS discussed above, these other
13 emails were either entirely blank or contained nothing more than a subject header, and some
14 of these emails were stored in the “Drafts” folder on Rosenberg’s email account.

15 62. There is probable cause to believe that SUBJECT ACCOUNT 87 was an email
16 account that the user of SUBJECT ACCOUNT 86 used in order to send promotional emails,
17 which advertised the services he provided through the payment of commercial bribes to
18 corrupted Amazon employees and contractors. Investigators found such promotional emails
19 in Rosenberg’s email account, including this email:
20
21
22
23
24
25
26
27
28

FLASH SALE Extended....50% OFF + \$399 Any Category OFFER

From: [REDACTED]
 To: reinstatement911@mail.com
 Date: Mon, 02 Dec 2019 18:00:49 -0800

Hello,

Hope you had a Nice Thanksgiving and a crazy black Friday shopping as well. We have received lot of emails and facebook messages requesting us to extend the **FLASH SALE** for another 24 Hours.

Here is your CHANCE to get approvals under Amazon's Restricted categories with our team's Help.

Last Evening we have obtained lot of Beauty Topicals, Baby Topicals, Dietary Supplements, Lighting, Pet Care and other categories approvals too.

We are making Amazon Support team to work 24*7 for us to get the approvals as soon as possible. :)

63. Investigators have not identified any payments by Rosenberg to the user(s) of SUBJECT ACCOUNTS 86 and 87, though this aspect of the government's investigation is ongoing. The government has, however, identified payments by another subject of the investigation who operates a third-party merchant account on the Amazon Marketplace to a PayPal account registered to [REDACTED]. This payment establishes additional probable cause to believe that the user of SUBJECT ACCOUNTS 86 and 87 solicited its services to Amazon third-party merchants, and their representatives.

SUBJECT ACCOUNT 88

- [REDACTED] ("SUBJECT ACCOUNT 88")

64. There is probable cause to believe that [REDACTED] ("SUBJECT ACCOUNT 88") will contain evidence of the crimes under investigation. Records produced by PayPal show that an account registered under SUBJECT ACCOUNT 88 is assigned to a user who provided the name "[REDACTED]" and a street address in Brooklyn, NY. According to PayPal records, between January 1, 2017, and September 1, 2020, that PayPal account sent over \$370,000 to various recipients and also received more than \$14,000. The

1 amounts received by the PayPal account registered to SUBJECT ACCOUNT 88 included a
 2 \$100 transfer from the reinstatement911 PayPal account on or about December 25, 2018 and
 3 a \$300 transfer from the PayPal account registered to effyrosenberg[@]gmail.com on or
 4 about December 26, 2018.

5 65. In addition to receiving payment from Rosenberg, the PayPal account
 6 registered to SUBJECT ACCOUNT 88 also transferred thousands of dollars to the PayPal
 7 accounts registered to SUBJECT ACCOUNTS 80 and 81.

8 66. Investigators found five emails to/from SUBJECT ACCOUNT 88 in
 9 reinstatement911[@]mail.com, all of which were stored in the "Drafts" folder of
 10 Rosenberg's email account. Three of the emails contained no content (i.e., no subject line
 11 and no text). The other two emails are shown below, and appear to discuss the performance
 12 of tasks in connection with merchant identification numbers for 3P Seller accounts that
 13 ROSENBERG provided in the subject lines of those emails (as he did in connection with
 14 other emails):

15 Re: [REDACTED]

16
 17 From: John Smith <reinstatement911@mail.com>
 18 To: [REDACTED]
 19 Date: Sat, 26 Jan 2019 21:01:30 -0800

20
 21 Sent: Sunday, January 27, 2019 at 12:00 AM
 22 From: [REDACTED]
 23 To: "John Smith" <reinstatement911@mail.com>
 24 Subject: Re: A3EZ11F0WNJAM8

25 payment?

26 On Fri, Jan 25, 2019 at 9:23 AM John Smith <reinstatement911@mail.com> wrote:
 27
 28

Re: [REDACTED]

From: John Smith <reinstatement911@mail.com>
 To: [REDACTED]
 Date: Wed, 26 Dec 2018 16:09:44 -0800

Sent: Wednesday, December 26, 2018 at 12:40 PM
 From: [REDACTED]
 To: "John Smith" <reinstatement911@mail.com>
 Subject: Re: [REDACTED]
 send paypal

On Wed, Dec 26, 2018 at 12:36 PM John Smith <reinstatement911@mail.com> wrote:

67. Based on the foregoing, I respectfully submit that there is probable cause to believe that SUBJECT ACCOUNT 88 was used by an individual who performed the same types of services for Rosenberg that the users of the other SUBJECT ACCOUNTS performed. Although the emails found in reinstatement911[.]mail.com do not discuss the precise work that the user of SUBJECT ACCOUNT 88 performed, they do reflect the same conveyance of a merchant identification number and references to payment.

SUBJECT ACCOUNT 43 and SUBJECT DEVICES

- nishadkunju[.]icloud.com ("SUBJECT ACCOUNT 43")
- 128 GB SanDisk Thumb Drive, 1 TB WD Hard Drive, and Black iPhone 8 Plus, all seized from [REDACTED], India ("SUBJECT DEVICES")

68. There is probable cause to believe that the content of Kunju's Apple iCloud account, registered in his name, will include evidence of criminal activity undertaken by him and others. Records produced by Apple show that an iCloud account (ID 12029276684), was created in March 2018, registered to nishadkunju[.]icloud.com under the name "Nishad Kunju" and address [REDACTED] India. The Apple records also show

1 that the account had activated the iCloud Backup and iCloud Drive features, as well as
2 Contacts and Notes, among other things, and that the account was in “active” status. Apple
3 records show Kunju’s use of various Apple devices, including multiple iPhones and an
4 Apple Watch S3. Further iCloud log activity records for Kunju’s iCloud account show
5 regular service of an iPhone X (10) and backups through April 15, 2020.

6 69. Kunju was involved in many aspects of the criminal scheme, including
7 misappropriating Amazon’s proprietary data. At the outset of this investigation, Amazon’s
8 counsel informed investigators that as part of an internal investigation by Amazon, Amazon
9 interviewed Kunju about his work with Joseph Nilsen. According to Amazon’s attorneys,
10 Kunju confessed that Nilsen had provided kickbacks to him and many other employees in
11 Amazon. Kunju also told Amazon that Nilsen worked with former Amazon employees,
12 including Rohit Kadimisetty (who was charged in the Indictment and has since pleaded
13 guilty to Conspiracy to Commit Violations of the Travel Act for his participation in the
14 commercial bribery conspiracy). Kunju informed Amazon that Nilsen provided kickbacks to
15 help third-party sellers in a number of ways, including by providing data of
16 suspended/blocked sellers, providing annotations and related information for blocked sellers,
17 and helping with reinstatement of blocked seller accounts. Kunju stated that he
18 communicated with Nilsen via email and with Nilsen and others involved in the scheme via
19 WhatsApp. Kunju also provided Amazon with copies of communications related to his
20 criminal conduct, and Amazon provided copies to investigators.

21 70. Communications collected in the course of the investigation confirm Kunju’s
22 participation in misappropriating information from Amazon in exchange for bribes. For
23 example, WhatsApp communication records show that on or around June 20, 2018, Nilsen
24 and Kunju used WhatsApp to discuss how Kunju had shared “hell lot of wikis on
25 searchability” of product listings in the Amazon Marketplace. In response, Nilsen said:
26 “Can you grab some Wiki’s for me so I can ensure I know how all of these elements work
27 and these accounts are flawless?” According to Amazon, Wikis “contain confidential
28 information about Amazon capabilities, metrics, Seller disciplinary enforcement thresholds,

1 and how to navigate Amazon's data-driven system." Amazon has explained that "[w]ith
2 access to various wikis, a Seller can circumvent Amazon's guidance on addressing Seller
3 malfeasance, understand Amazon's proprietary methods for ranking Sellers and products,
4 and gain a competitive advantage over other sellers."

5 71. Chats between Nilsen and Kunju also refer to the commercial bribes that
6 Nilsen paid for access to Amazon's proprietary information, including its Wikis. For
7 instance, in a WhatsApp chat on or around July 3, 2018 (when Kunju still worked at
8 Amazon), Nilsen told Kunju to ask [REDACTED] (who also worked at Amazon and
9 was also later terminated by Amazon as part of its internal investigation) to gather wikis
10 from Amazon's servers and proposed to Kunju the following terms of payment: "2k the last
11 day of the month as agreed? Or if you feel the need to renegotiate that is fine too."

12 72. Records received from the online payment service Remitly show that a
13 Remitly account registered in Kristen Leccese's name was used to send \$2,000 directly to
14 [REDACTED] on or about July 22, 2018. Investigators have identified additional payments to
15 Kunju and [REDACTED] during this time frame.

16 73. Kunju also exchanged WhatsApp communications with Nilsen about collecting
17 annotations. For example, in a string of WhatsApp messages that Amazon collected and
18 produced to investigators, Nilsen texted Kunju on April 8, 2018, asking "Do you think you
19 can grabe these annotations? +200" and then adding "[REDACTED]." Kunju
20 responded, "Uk or us?" Joe answered, "US," and Kunju wrote back, "Cool" and then,
21 "Sending in five min." Kunju then wrote, "Sent."

22 74. After Kunju was terminated by Amazon in or around August 2018, Nilsen
23 continued to acquire confidential information from Amazon's computer systems through the
24 use of other Amazon employees, including [REDACTED], often by working with Kunju, who had
25 connections to Amazon employees. Records obtained over the course of the investigation
26 establish that, even after his termination by Amazon, Kunju used WhatsApp to communicate
27 with Nilsen about the scheme under investigation.
28

75. In the days after his and other employees' termination, Kunju used WhatsApp to warn Nilsen about potential future enforcement actions by Amazon. For instance, on or about September 4, 2018, Kunju warned Nilsen that Amazon "is now going further to clients," and proceeded to name various client accounts that are suspected to have benefited from the commercial bribery scheme. In the course of that online chat, Nilsen instructed Kunju to "delete" any stored messages between Kunju, on the one hand, and Nilsen, Leccese, and Kadimisetty, on the other hand. Kunju agreed to do so. Kunju then told Nilsen, "I still wish to work with you bro," and Nilsen responded, "Same dude." Approximately one month later, on or about October 19, 2018, Kunju began a new WhatsApp chat with Nilsen under a different telephone number and the aliases "Jonathan Li" and "Tina," and sent Nilsen a message stating, "New number bro."¹³

76. And Kunju did continue to work with Nilsen to misappropriate information from Amazon and bribe Amazon employees. For example, Kunju used WhatsApp to communicate with Nilsen about using Amazon insiders to attack 3P seller accounts owned by competitors of Nilsen and/or his clients. On or about October 18, 2019, Nilsen sent Kunju a WhatsApp message stating: "This fucking [REDACTED] account – if we take it out we split 60 g's with that guy 15k each." I believe that the reference to "60 g's" is a reference to the amount that Nilsen expected to receive from a client in exchange for "tak[ing]" out the competing "[REDACTED] account." Based on other records obtained over the investigation, I have probable cause to believe that the term "[REDACTED] account" referred to a 3P seller account belonging to a seller named "[REDACTED]"¹⁴ Between October 2018 and January 2019, Nilsen and Kunju discussed techniques for attacking the [REDACTED] account. For instance, Kunju said, "We are trying to block the seller with allegations of review

¹³ In emails and online chats, Nilsen, Leccese, Nuhanovic, and other suspected members of the conspiracy referred to Kunju by the nickname "Tina." I have not found chats in which any other person was referred to as "Tina." Furthermore, Amazon identified "Tina" as a known nickname of Kunju. The substance of the communications themselves, including discussions regarding his termination and the transfer of funds, make clear that Kunju is the user of the new WhatsApp account.

¹⁴ The records I rely on in forming this belief include other chats, such as a chat between Nuhanovic and Nilsen on or around March 16, 2019, in which Nuhanovic sent Nilsen a hyperlink to the Amazon storefront for [REDACTED], with a note saying "[REDACTED] growing."

manipulation right?” and proceeded to state “I have a good plan if we are going after review manipulation.” In my review of other records from this investigation, I believe that the phrase “allegations of review manipulation” refers to a process by which Kunju and/or others acting at his direction placed positive reviews on a targeted 3P Seller account without the 3P seller’s knowledge, and then lodged a complaint with Amazon that the 3P Seller used those reviews to boost its sales.

77. Kunju described how he could ensure that the phony reviews on [REDACTED]’s seller page would not be traced back to Kunju, but instead falsely would be traced back to [REDACTED], thus making it appear as if [REDACTED] were posting positive reviews to its on page in violation of Amazon’s terms of service. Kunju proposed “hack[ing] into” the “competitors ip” and “post[ing] few reviews on his own products,” noting that such a strategy could be “game.” In response, Nilsen suggested using “known offenders”—i.e., third parties known to Amazon who 3P Sellers retain to manipulate reviews: “Wouldn’t it be easier to use the known offenders who Amazon still allows to keep their buyer accounts even though they have been ratted out on multiple POAs lol.” Kunju thereafter proposed posting reviews from accounts that bore names and addresses associated with [REDACTED], in order to dupe Amazon into attributing the reviews to [REDACTED] and disciplining [REDACTED] for violating Amazon’s rules against posting positive reviews to one’s own seller account. Nilsen noted that, in order to carry out the contemplated scheme, an Amazon insider would need to collect information about [REDACTED]: “We will need soldier to grab info of current business info/name on file.” Kunju responded: “Absolutely.” Based on the records collected in this case, I believe that Nilsen and Kunju sometimes used the word “soldier” to refer to [REDACTED], who was an Amazon employee at the time of this text conversation. The government is continuing to investigate the precise steps that the members of the conspiracy took in order to carry out the contemplated attack against [REDACTED].

78. There is also probable cause to believe that Kunju used WhatsApp in furtherance of the payment of commercial bribes to Amazon employees. For instance, on or about November 3, 2018, Kunju told Nilsen that “Soldier completed work. . please send

1 soldiers funds,” and stated “My soldier wants money so please bring in as many jobs u can.”
 2 Later that day, Nilsen and Kunju communicated through WhatsApp about establishing bank
 3 accounts under other names, and accessing those accounts from different computers. Nilsen
 4 and Kunju also discussed how to limit the amount of money sent in any one transaction, with
 5 Nilsen asking, “[w]hat is the most amount of money that we can send to you through bank,”
 6 and Kunju responding, “No limit I guess but less than 5k per account would be safe.”

7 79. Kunju then used WhatsApp to provide Nilsen with two bank accounts into
 8 which Nilsen could deposit funds: one account in the name “N [REDACTED] S” and the other
 9 account in the name “R [REDACTED] P [REDACTED].” A Chase Bank account registered to Digital
 10 Checkmate made transfers to N [REDACTED] S and R [REDACTED] P [REDACTED] throughout November 2018. The
 11 memo lines for those transfers refer to them as a purported “wedding gift” and a purported
 12 “loan.” Using the email address freakdaze[.]gmail.com,¹⁵ Kunju received emails from the
 13 address [REDACTED], one of which attached a bank statement that
 14 purported to show substantial incoming and outgoing financial transfers from an account
 15 registered to [REDACTED]. The cover email to Kunju from “R [REDACTED]
 16 P [REDACTED],” which attached the bank statements, is as follows:

17
 18
 19
 20
 21
 22
 23
 24
 25
 26
 27 ¹⁵ Based on numerous records in this case, I believe that the email account freakdaze[.]gmail.com was used by Kunju.
 28 For example, in a WhatsApp exchange between Kunju and Nilsen on June 10, 2018, Nilsen and Kunju discussed getting
 information about an Amazon account. Nilsen then wrote, “I am going to have a friend send funds through paypal
 shortly . . . I am giving him the cash. What’s the best email?” Kunju wrote back, “freakdaze@gmail.com.”

Fwd: 531295741_May2019.pdf

From: Nishad Kunju <freakdaze@gmail.com>
 To: [REDACTED]@gmail.com
 Date: Fri, 14 Jun 2019 08:33:56 -0700
 Attachments: 531295741_May2019.pdf (82.43 kB)

----- Forwarded message -----
 From: R [REDACTED] P [REDACTED] <[REDACTED]@gmail.com>
 Date: Mon, 10 Jun 2019 at 8:49 PM
 Subject: Fwd: 531295741_May2019.pdf
 To: <freakdaze@gmail.com>

80. There is probable cause to believe that Kunju's iCloud backup and drive features would save copies of WhatsApp chats to his iCloud remote-storage account. As noted above, Apple records show that Kunju had activated his iCloud Backup and Drive features, which would enable the user to access those files and chats from multiple devices registered to the same iCloud account, unless the user took steps to prevent those backups from being created. The iCloud Drive and iCloud Backup features also save other materials, including the types of digital files that the suspected members of the scheme are believed to have used in furtherance of the scheme, such as spreadsheets, business reports, product listings, and proprietary files that were misappropriated from Amazon's network.

81. This affidavit also seeks authorization to search Kunju's digital devices, including an iPhone. In 2020, based on a Mutual Legal Assistance Treaty (MLAT), investigators prepared a Request for Assistance and served it on Indian officials. The request asked Indian officials to interview certain individuals and conduct searches in accordance with Indian Law. One of the individuals named in the MLAT was Nishad Kunju. In May 2021, the United States Attorney's Office for the Western District of Washington received a response to that MLAT. It included a letter from the Office of the Superintendent of Police and Central Bureau of Investigation (CBI) in New Delhi. The response included a report stating, "in order to execute the instant MLAT . . . searches have been conducted in the

1 following 08 premises: i. Sh. Nishad Kunju [REDACTED]
 2 [REDACTED] Hyderabad.” The report also listed other locations
 3 that had been searched. The report further listed “the documents & articles so recovered,”
 4 and below a header stating “Mr. Nishad Kunju & [REDACTED], [REDACTED],
 5 [REDACTED],” the report
 6 listed (1) “San Disk Pen Drive 128GB Crazer Blade,” (2) “Hard disk – WD make – 1.0 TB
 7 WD10JPVX; S/N: WXW1A48H78YN,” (3) “I phone – IS13252/IEC 60950-1; IS16333
 8 (Part 3, R-4103730 along with Airtel 4G Sim – 128K.” Included in the response was an
 9 attestation from Inspector Rahul Tamatam under penalty of criminal punishment for false
 10 statement that the items had no change in condition while in his custody. The materials
 11 provided by the Indian Authorities indicate that the search and seizure from Kunju’s
 12 residence described in the reports occurred on or around February 21, 2021.

13 82. In response to the MLAT, Indian authorities provided reports as well as seized
 14 documents and devices, including the SUBJECT DEVICES. The materials provided by CBI
 15 also included an index numbering and detailing all the items seized and produced via the
 16 MLAT, including items seized from Kunju's residence. All of these items, including the
 17 SUBJECT DEVICES, are currently stored in FBI evidence control in Seattle Washington
 18 and are labeled accordingly.

19 83. The materials received from Indian authorities also included a report
 20 describing an interview with Nishad Kunju. The report from that interview indicates that,
 21 among other things, Kunju admitted that he worked with Nilsen to prepare plans of action
 22 and received payment for his work. The report also indicates that Kunju said he “didn’t
 23 directly helped (sic) Nilsen in reinstating any seller account.”

24 84. Although many of the specific communications described above occurred
 25 between 2018 and 2019, investigators identified several communication threads between
 26 Nilsen and Kunju via WhatsApp and email well into 2020. There is probable cause to believe
 27 that evidence of those communications and the subject matter that they concern will continue
 28 to be found on SUBJECT ACCOUNT 43 and the SUBJECT DEVICES.

SUBJECT ACCOUNT 51

- The Facebook account bearing digital sign identifier [REDACTED] (“SUBJECT ACCOUNT 51”)

85. SUBJECT ACCOUNT 51 was used by Rosenberg in furtherance of the scheme under investigation. Records produced by Facebook show that SUBJECT ACCOUNT 51 was registered by “Ed Rosenberg” on or about November 24, 2010 under the email address “effyzaz[@]gmail.com.” Other records found in this investigation show that effyzaz[@]gmail.com is an email address used by Rosenberg in connection with his consulting business, Effyzaz. When registering SUBJECT ACCOUNT 51, Rosenberg provided the street address “[REDACTED] Brooklyn, NY,” which is Rosenberg’s home address.

86. Records found in Nilsen’s and Leccese’s¹⁶ Facebook accounts show that Nilsen, Leccese, and Rosenberg communicated over Facebook regarding 3P consulting, including consulting projects that involved the payment of bribes to Amazon employees. In my review of these communications, I developed probable cause to believe that Rosenberg, Nilsen, and Leccese often used multiple means of electronic communication to carry on a conversation about a single topic. For instance, when discussing a particular project, Nilsen and Rosenberg would communicate via both email and Facebook Messenger, as well as by telephone. Thus, when describing examples of Rosenberg’s use of Facebook in furtherance

¹⁶ Based on my review of records in this case, I am aware that Leccese is Nilsen’s girlfriend and business associate, and has been in those roles for substantially the amount of time relevant to this case. Leccese is suspected to have engaged in numerous acts of fraud and dishonesty over the course of the scheme, including submitting forged invoices to Amazon when seeking Amazon’s approval to sell products in certain restricted categories. On or about August 19, 2019, I interviewed Leccese at her and Nilsen’s shared residence in New York, which agents were searching pursuant to a search warrant. During that interview, Leccese admitted to paying bribes to Amazon employees in India. Leccese further stated her belief that Rosenberg paid bribes to Amazon employees in Seattle, though she did not present hard proof of such bribes – e.g., by claiming to have seen such bribes or heard directly from Rosenberg about the fact or amounts of such bribes. Leccese did tell investigators that she purportedly had seen internal Amazon annotation records referring to so-called “Ed escalations”—i.e., multiple 3P sellers used Rosenberg to communicate with Amazon about enforcement activity against their accounts. In May 2022, Leccese pleaded guilty to Conspiracy to Violate the Travel Act for her participation in the commercial bribery scheme.

1 of the scheme, I refer to communications via other electronic applications where necessary to
2 provide context.

3 87. Below are three examples of how Rosenberg used SUBJECT ACCOUNT 51
4 to communicate with Nilsen about the scheme and conduct under investigation.

5 88. **First**, on or about June 26, 2018, Nilsen emailed Rosenberg under the subject
6 line: “**Two-Fer Tuesdays – Exclusive deal for Mr. Ed Rosenberg”:

7 Hello Ed,

8 This is a week where friends are covering for non-friends and basically, right now
9 notice is filled up with a bunch of friends. I know there are psyched about how much
10 easier it will be. I’m not sure if it is because nobody will be around them to question
11 them making it easier or because of the volume that they can do. They said they
12 would start with 6 sellers who are suspended for anything to do with notice/copyright
13 etc. For this once in a lifetime deal, you can take any prices that I have given you for
14 notice and slice it completely in half. This is like a lightning deal on crack. The only
15 terms are is that you must supply 3 or more sellers. To be clear, this is Kobe laying it
16 up and Shaque [*sic*] coming in to crush the backboard. If approved, all cases will be
17 slammed dunk. In addition to this service, we are offering a charge of \$2,000 and you
18 have your entire record swiped clean ALL previous TM violations policy warnings
19 and RO complains [*sic*] will be sent to never neverl [*sic*] land.

20 89. Based on my review of records regarding the operation of the Amazon
21 Marketplace, I am aware that “notice” is a term typically used to refer to a department within
22 Amazon that controls the automated email address notice@amazon.com. That email address
23 is used by Amazon to communicate with 3P Sellers about intellectual property claims that
24 they make against other sellers or that other sellers make against them. Thus, there is
25 probable cause to believe that Nilsen’s email conveyed to Rosenberg that certain
26 compromised Amazon employees in Amazon’s “notice” department were “on the clock” and
27 available to provide beneficial treatment to Rosenberg’s 3P clients in exchange for bribes.

28 90. Following Nilsen’s initial email, Rosenberg and Nilsen engaged in this email
exchange over the following hour:

ROSENBERG: lol – this week only – and just notice – right?

NILSEN: Ohhh man Ed – what a Negative Nancy response. Regarding this week
only – I can’t say it won’t happen again but the first time since I’ve known this. It is

for only for the day that we pretty much have control of notice@. They are covering for the week, but there is always one buzzkill. These guys are all aligned today and are ready to liberate the world. This day ONLY. But we are fortunate to have even one day. And yes, though our reach has extended greatly and increased our odds tremendously, I still have yet to find my magic wand for the other departments. Getting closer, though, I will tell you. Lemmmmmeeee knowwwwww.

ROSENBERG: [REDACTED]

¹⁷

¹⁸

¹⁹ – maybe more

NILSEN: I'll get a quote now sir – I am eying that one that ends in WN – 10k discount can't complain about that.

91. Approximately one week later, on or about July 3, 2018, Rosenberg sent a follow-up email to Nilsen asking whether “these prices still stand?” Rosenberg then used SUBJECT ACCOUNT 51 to engage in the following exchange with Nilsen (excluding extraneous messages regarding other subjects):

ROSENBERG: The 3 accounts.. i emailed u

NILSEN: Two-fer Tuesdays ... combo deal. You cant cherrypick and confirm one by one.

ROSENBERG: [Thank you.] will check it out.

ROSENBERG: If I do 2, can do

ROSENBERG: Can do the accounts? Ok, but can do the accounts?

NILSEN: Yeah ... there are 3 notice guys that are needed to do what they do ... one of them has one week off. He'll be back in 2-3 days. We can 100% def do it, though.

¹⁷ Based on my review of other communications and documents in this investigation, I believe this merchant identification number relates to an Amazon Marketplace account operating under the trade name “[REDACTED]”. I understand, from other records in this case, that “RO” is typically used in the context of the Amazon Marketplace to refer to “Rights Owner” complaints—i.e., where a purported intellectual property rights owner alleges that a 3P seller is infringing those rights.

¹⁸ Based on my review of other communications and documents in this investigation, I believe this merchant identification number relates to an Amazon Marketplace account operating under the trade name “[REDACTED]”.

¹⁹ Based on my review of other communications and documents in this investigation, I believe this merchant identification number relates to an Amazon Marketplace account operating under the trade name “[REDACTED]”.

1 When he gets back, we'll still honor all deals and prices/mindset for these three
2 accounts.

3 92. On or about July 8, 2018, Nilsen sent a message to SUBJECT ACCOUNT 51
4 stating "notice is back [from] vacation." He then asked Rosenberg to "email me the first two
5 Merch I.D.'s please?" and Rosenberg responded: "just notice right --." Nilsen responded
6 "Slam dunk 100% -- just notice."

7 93. **Second**, Rosenberg communicated with Nilsen about the reinstatement of a 3P
8 seller who Nilsen referred to Rosenberg. Specifically, in or about early February 2019, J.P.
9 (the operator of a 3P seller account) sent Nilsen a message over Facebook asking for help
10 reinstating his seller account, which he claimed Amazon had wrongly suspended. After
11 determining that his own contacts inside Amazon could not assist with the account's
12 reinstatement, Nilsen referred [REDACTED] to Rosenberg.

13 94. On or about February 3, 2019, [REDACTED] told Nilsen that "Ed should be meeting with
14 Amazon @ noon tomorrow and give me an update after. ... he said he has a call with
15 someone tomorrow at noon." At around the time of that message from [REDACTED], Rosenberg sent
16 Nilsen a message from SUBJECT ACCOUNT 51, stating: "tell [REDACTED] to sit tight -- pulling all
17 strings for him -- would love today but my guess is its coming." When Nilsen asked
18 Rosenberg about Rosenberg's confidence that [REDACTED]'s account would be reinstated, Rosenberg
19 responded from SUBJECT ACCOUNT 51 "if this is the story -- yes very high -- very very."

20 95. On or about February 5, 2019, [REDACTED] sent Nilsen the screenshot of an apparent
21 email from Rosenberg to [REDACTED]:

22 Subject: Re: You have a new lead from a form - Suspended Account

23 [REDACTED] Hi - ok - spoke again to the lady and she said the case will be reviewed latest Wednesday - I am hoping before - she did not look at your case yet
24 but said it makes sense
25 that you would be locked out for something like this and its a flaw in the system that they need to fix. I explained that this does not help us today and we need help right
26 now. She said wed latest
27 The email you just sent will make some noise

28 96. Other evidence suggests that the "lady" to which Rosenberg referred in this
email was [REDACTED], who at the time of the relevant conduct was a manager at Amazon.

Specifically, telephone records produced by Rosenberg's cellular telephone provider show that Rosenberg conducted a 55-minute phone call with a personal cellular telephone registered to a person believed to be [REDACTED]'s husband. After sending Nilsen the screenshot of Rosenberg's email, [REDACTED] further stated: "He met with Amazon contact, she acknowledged it's a flaw in their system and they'll review by Wednesday at the latest. He has me send the below email to get more eyeballs on it..."

97. [REDACTED] then shared with Nilsen the image of an email that [REDACTED] sent to the email account associated with Jeff Bezos, the CEO of Amazon. Nilsen responded to [REDACTED] that he was "FUCKING PIST" because Rosenberg was "talking to that lady – that's not the big person I recommended him for you for." I interpret Nilsen's message to mean that Nilsen understood Rosenberg to have more than one internal contact at Amazon, including [REDACTED] and someone other than [REDACTED] who was a "big person."

98. On or about February 6, 2019, Nilsen informed [REDACTED] that Rosenberg had secured the reinstatement of [REDACTED]'s seller account on Amazon. Following that exchange, Rosenberg sent Nilsen messages from SUBJECT ACCOUNT 51, as well as emails, regarding the reinstatement. For instance, in a series of emails, Rosenberg noted that J.P.'s account may not have been reinstated completely, and then told Nilsen to "do nothing – being worked on." Minutes later, Rosenberg stated "back for good."

99. *Third*, there is probable cause to believe that Rosenberg used SUBJECT ACCOUNT 51 to communicate with Leccese regarding the submission of fictitious documentation to Amazon. For example, in chats between SUBJECT ACCOUNT 51 and Leccese's Facebook account, Leccese and Rosenberg discussed the submission of forged invoices to Amazon when seeking approval to sell in certain categories. Leccese explained: "It is an ugly phrase 'forge' ... I feel like people are forced to do these things. How else to survive in this circus. Rosenberg responded: "yep – agree."

SUBJECT ACCOUNT 89 and 90

- [REDACTED] ("SUBJECT ACCOUNT 89")

- amzLamarnt[@]mail.com (“SUBJECT ACCOUNT 90”)

100. Evidence gathered during this investigation shows that Rosenberg paid bribes to an Amazon employee named [REDACTED]. According to an Amazon internal document recovered from Nilsen’s iCloud account, which was dated June 26, 2018 and marked “Amazon Confidential” (and which I suspect was improperly obtained through the conduct under investigation), [REDACTED] was identified as a member of a “Product Review Abuse team” responsible for “thoroughly investigat[ing] all reports of product review abuse and/or manipulation across all marketplaces.” Other public sources corroborate [REDACTED]’s position at Amazon during this approximate time period, until in or about December 2018.

101. As described above, Rosenberg registered a PayPal account in the name of “Tom Landry” using his email account reinstatement 911[@]mail.com. According to PayPal records for that account, between in or about April 2018 and in or about December 2018, that PayPal account transferred a total of approximately \$18,650, in thirty-three (33) separate transactions, to a PayPal account belonging to [REDACTED], who was employed at Amazon during that time period.

102. According to records obtained from PayPal, this recipient account was registered in [REDACTED]’s name, under the business name “MW Interpretation and Translation,” using email address [REDACTED] (SUBJECT ACCOUNT 89). The account was created on April 26, 2020.

103. The incoming payment transaction log, an excerpt of which is displayed below,²⁰ confirmed the regular (near weekly) payments from a PayPal account in the name of “Tom Landry” associated with email reinstatement911[@]mail.com (Rosenberg’s PayPal account described above):

²⁰ Certain categories of transaction information are not displayed in the chart for use in this affidavit. Further, contact information for unrelated transfers have been redacted.

Transaction Log												
Date	Time	Time Zone	Name	Type	Status	Subject	Currency	Gross	Fee	Net	From Email Address	To Email Address
8/5/2020	11:50:26 AM	America/Los Angeles		Credit Card Payment Received (Pa	Completed	~(C)-CLD-150185800~	USD	\$300.00 USD	\$0.00 USD	\$300.00 USD		
4/1/2020	7:32:08 AM	America/Los Angeles		Mass Payment Received	Completed		USD	\$508.50 USD	\$0.00 USD	\$508.50 USD		
3/16/2020	7:01:53 PM	America/Los Angeles		Mobile Express Checkout Payment	Refunded	~(C)-CLD-1502931200~	USD	\$37.75 USD	-\$1.30 USD	\$36.45 USD		
1/3/2020	4:18:41 AM	America/Los Angeles		Instant Transfer Received (Personal)	Completed	~(C)-CLD-1578473000~	USD	\$508.44 USD	\$0.00 USD	\$508.44 USD		
12/21/2019	10:17:39 AM	America/Los Angeles		Credit Card Payment Received	Completed	~(C)-CLD-1578207400~	USD	\$201.94 USD	\$9.18 USD	\$192.76 USD		
11/20/2019	10:38:37 PM	America/Los Angeles		Mobile Express Checkout Payment	Completed	~(C)-CLD-1574888300~	USD	\$34.14 USD	-\$1.29 USD	\$32.85 USD		
11/12/2019	3:02:16 PM	America/Los Angeles		Mobile Express Checkout Payment	Completed	~(C)-CLD-1574298900~	USD	\$110.26 USD	-\$3.60 USD	\$106.66 USD		
12/8/2019	8:56:17 PM	America/Los Angeles	Tom Landry	Credit Card Payment Received (Pa	Completed		USD	\$300.00 USD	\$0.00 USD	\$300.00 USD	reinstatement911@gmail.com	
11/24/2019	7:57:27 PM	America/Los Angeles	Tom Landry	Credit Card Payment Received (Pa	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
11/18/2019	7:34:16 AM	America/Los Angeles	Tom Landry	Credit Card Payment Received (Pa	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
11/11/2019	8:32:15 AM	America/Los Angeles	Tom Landry	Credit Card Payment Received (Pa	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
11/4/2019	7:54:59 PM	America/Los Angeles	Tom Landry	Credit Card Payment Received (Pa	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
10/29/2019	8:25:45 AM	America/Los Angeles	Tom Landry	Credit Card Payment Received (Pa	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
10/20/2019	8:67:02 PM	America/Los Angeles	Tom Landry	Credit Card Payment Received (Pa	Completed	~(C)-CLD-1540892800~	USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
10/13/2019	8:32:26 PM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed	~(C)-CLD-1539932400~	USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
10/7/2019	8:24:52 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
9/30/2019	7:01:46 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
9/23/2019	7:56:41 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
9/16/2019	1:04:28 PM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed	~(C)-CLD-1537426800~	USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
8/9/2019	8:51:52 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
8/2/2019	4:44:53 PM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed	~(C)-CLD-1536333400~	USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
8/27/2018	3:42:08 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed	~(C)-CLD-1530698800~	USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
8/20/2018	8:41:55 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed	~(C)-CLD-1530007400~	USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
8/13/2018	4:14:26 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed	~(C)-CLD-1534489200~	USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
8/6/2018	8:23:19 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
7/30/2018	8:07:35 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
7/23/2018	4:44:36 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
7/15/2018	7:16:36 PM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed	~(C)-CLD-1532070000~	USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
7/9/2018	9:52:00 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
7/1/2018	9:45:02 PM	America/Los Angeles	Tom Landry	Credit Card Payment Received (Pa	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
6/24/2018	12:24:59 PM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
6/15/2018	8:12:28 PM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
6/11/2018	10:34:42 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
6/7/2018	3:27:34 PM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
6/25/2018	12:23:02 PM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
6/19/2018	11:35:13 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
6/11/2018	11:07:16 AM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
6/4/2018	2:50:46 PM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$600.00 USD	\$0.00 USD	\$600.00 USD	reinstatement911@gmail.com	
4/27/2018	2:12:25 PM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$250.00 USD	\$0.00 USD	\$250.00 USD	reinstatement911@gmail.com	
4/28/2018	3:01:47 PM	America/Los Angeles	Tom Landry	Payment Received (Personal)	Completed		USD	\$100.00 USD	\$0.00 USD	\$100.00 USD	reinstatement911@gmail.com	

Notably, the first incoming transfer occurred on April 26, 2020, the same date the [REDACTED] PayPal account itself was created. The initial incoming transfer was in the amount of \$100 and came from Rosenberg's reinstatement911 PayPal account. A \$250 transfer followed the next day. Thereafter, with the exception of the final \$300 transfer on December 6, 2018, payments were in the amount of \$600. Further noteworthy, the payments from the reinstatement911 PayPal account ceased in December 2018, which, according to public source information, approximates the date when [REDACTED] left her position at Amazon.

104. Based on my training and experience and involvement in this investigation, I believe that these payments to [REDACTED] from Rosenberg's reinstatement911 PayPal account constitute illicit bribes for internal information and assistance in gaining unfair competitive advantages on the Amazon Marketplace. I also believe that this [REDACTED] PayPal account was created for the purpose of receiving illicit payments and that its association with interpretation and/or translation services²¹ was pretextual, an attempt to disguise the true, illegal nature of the payments from Rosenberg.

105. According to transaction records for the [REDACTED] PayPal account, the account holder ([REDACTED]) made numerous (approximately weekly) transfers of funds to her linked

²¹ [REDACTED] is believed to be a Spanish speaker and has provided Spanish-language interpretation and translation services.

1 bank account, at BECU, between on or about June 7, 2018, and December 7, 2018. Most
2 were in the amount of \$600, the same amount regularly paid to her from the
3 reinstatement911 PayPal account.

4 106. The [REDACTED] PayPal account is associated with a bank account at BECU,
5 ending in -9803. According to account records obtained from BECU, which is based in
6 Western Washington, this account ending in -9803 belongs to [REDACTED] and also is associated
7 with email address [REDACTED] (SUBJECT ACCOUNT 89). On the
8 membership application paperwork, which were dated in October 2017, [REDACTED] further
9 indicated that she was employed at Amazon in the fraud department. The BECU account
10 statements show \$600 transfers from the [REDACTED] PayPal account to [REDACTED]'s bank account,
11 as illustrated in the below excerpt from the monthly statement for the period of June 23,
12 2018, to July 27, 2018:

Deposits		
Date	Amount	Transaction Description
06/25	600.00	External Deposit PAYPAL TRANSFER - TRANSFER
06/29	1,709.48	External Deposit AMAZON.COM SVCS 4100075043 74 - DIRECT DEP
07/03	600.00	External Deposit PAYPAL TRANSFER - TRANSFER
07/11	600.00	External Deposit PAYPAL TRANSFER - TRANSFER
07/13	1,462.13	External Deposit AMAZON.COM SVCS 4100075043 74 - DIRECT DEP
07/18	600.00	External Deposit PAYPAL TRANSFER - TRANSFER
07/24	600.00	External Deposit PAYPAL TRANSFER - TRANSFER
07/27	1,395.29	External Deposit AMAZON.COM SVCS 4100075043 74 - DIRECT DEP
07/27	1.38	Dividend/Interest

13
14
15
16
17
18
19 107. Based on my training and experience, I know that PayPal account holders
20 typically receive account notifications, sent to the designated associated email account, of
21 certain account activity, including when an account is registered or created, when payments
22 are sent or received, and when accounts settings are modified. Accordingly, I believe there
23 is ample probable cause to believe that [REDACTED] (SUBJECT
24 ACCOUNT 89) will contain emails relating to a PayPal account used to facilitate the scheme
25 under investigation.

26 108. According to records obtained from Google, the account associated with
27 [REDACTED] (SUBJECT ACCOUNT 89) was opened in June 2017 and is
28 under the name "[REDACTED]":

GOOGLE SUBSCRIBER INFORMATION

Google Account ID: [REDACTED]
 Name: [REDACTED]
 e-Mail: [REDACTED]
 Alternate e-Mails:

Created on: 2017-06-29 16:08:51 UTC
 Terms of Service IP: 206.169.234.110

Services: Web & App Activity, Gmail, Location History, Google Calendar, Android, Google Hangouts, YouTube, Google Play, Tasks In Tingle, Google Play Music, Google My Maps, Google Maps, Google Payments, Google Docs, Google URL Shortener

Deletion Date:
 Deletion IP:

Last Logins: 2020-09-26 20:30:27 UTC, 2020-09-26 17:24:01 UTC, 2020-09-26 01:59:45 UTC

ACCOUNT RECOVERY

Recovery e-Mail: [REDACTED]
 Recovery SMS: [REDACTED]

PHONE NUMBERS

Signin Phone Numbers: [REDACTED]
 2-Step Verification Phone Numbers:

The account recovery email is [REDACTED]²² The account remained active through at least September 26, 2020 (the date Google conducted its query). I also note that this time period of account usage encompasses the criminal activity under investigation.

109. According to Google records, the account associated with recovery email [REDACTED] was created in July 2019 and is under the name "[REDACTED]" The recovery email is [REDACTED] (SUBJECT ACCOUNT 89), with which the account shares the same 206-area-code SMS recovery phone number, ending in -6610,²³ and multiple common IP address activity (logins using common IP addresses, which often is evidence of a common user). The last registered login for [REDACTED] was in March 2020.

110. On about October 7, 2020, investigators, including myself, interviewed [REDACTED] at her residence, located in or near Edmonds, Washington. After being advised that an interview was voluntary, [REDACTED] agreed to speak with investigators and did so outside her house. [REDACTED] confirmed that she formerly worked for Amazon for approximately four years. She stated that she started in vendor support and then moved to review investigations,

²² The name "[REDACTED]" is consistent with [REDACTED]'s name.

²³ This same phone number, ending in [REDACTED], also is a confirmed phone number linked to the [REDACTED] PayPal account that received payments from the reinstatement911 PayPal account discussed herein.

1 where he worked for about one and a half years before leaving the company. [REDACTED] further
2 confirmed her use of [REDACTED] (SUBJECT ACCOUNT 89) as the only
3 email she regularly used for several years.

4 111. When asked about the conduct under investigation, [REDACTED] admitted to
5 accepting bribes and payments from third parties related to her position within Amazon and
6 to providing internal information to assist sellers operating on the Amazon Marketplace.²⁴
7 According to [REDACTED], during her employment with Amazon, [REDACTED] met an individual at a
8 convention in Seattle who claimed to be an Amazon Seller. This individual was, she
9 believed, of Jewish background and from New York, but [REDACTED] could not remember his
10 name. This man asked [REDACTED] if she was interested in additional opportunities to make
11 money. [REDACTED] agreed, and the individual passed her email along to another person that used
12 the name “Tom Landry” (the name ROSENBERG used as an alias for a PayPal account, as
13 described above). In addition to email, [REDACTED] stated she also communicated with this
14 unknown individual via Instagram messages. [REDACTED] agreed to accept \$600 per week from
15 “Tom Landry” in exchange for help with his clients. “Tom Landry” would reach out to
16 [REDACTED] if he suspected his client was suspended for review manipulation. [REDACTED] would
17 then provide “Tom Landry” with information about why his client was suspended and what
18 they needed to do to get reinstated – for example, what would need to be written in the plan
19 of action. However, [REDACTED] claimed she never sent “Tom Landry” any internal Amazon
20 documents.

21 112. On October 9, 2020, [REDACTED] contacted Special Agent Howe both by telephone
22 and by email. [REDACTED]’s email to Special Agent Howe was sent from
23 [REDACTED] (SUBJECT ACCOUNT 89). [REDACTED] conveyed that she believed
24 that she communicated with email amzLamarnt@mail.com (SUBJECT ACCOUNT 90),
25 used by “Tom Landry”, however [REDACTED] stated she could not find any emails “related to
26 Tom.” [REDACTED] further stated that she believed that the person that she initially met at the
27

28 ²⁴ [REDACTED] initially denied any wrongdoing, but ultimately admitted to accepting bribes and assisting third parties related to her position within Amazon when presented with specific information obtained through the investigation.

1 convention who introduce her to “Tom Landry” was named “David,” but that she had
 2 minimal subsequent communications with him.²⁵

3 113. On about October 12, 2020, investigators obtained subscriber records from
 4 1&1 Mail for amzLamarnt@mail.com (SUBJECT ACCOUNT 90). The records, an excerpt
 5 of which is displayed below, establish that it is Rosenberg’s account:

6 amzlamart@mail.com

Customer Number	343262130
First/Last Name	ephraim rosenberg
Street	1446 E 27th St
Registration Date	2018-04-26 00:42
City / Zip Code	Brooklyn 11210
Country / Language	US / EN-US
Date of birth	1975-06-04 00:00
Status	Unlocked (barcode 0)
Alternative Email Address	effyzaz@gmail.com
Forwarding Address	

15 114. Specifically, the account is registered under the name “Ephraim Rosenberg”
 16 and a street address that aligns with Rosenberg’s known residence in Brooklyn, New York.
 17 The records also show that Rosenberg listed another one of his known email addresses
 18 (effyzaz@gmail.com) as the alternative email account for amzLamarnt@mail.com
 19 (SUBJECT ACCOUNT 90). Further, login activity included at least one IP address used to
 20 log into other accounts associated with Rosenberg.

21 115. Finally, according to account records, the registration date of the
 22 amzLamarnt@mail.com (SUBJECT ACCOUNT 90) account was April 26, 2018. As
 23 discussed above, on about the same date, the [REDACTED] PayPal account was created and
 24 received the first payment transfer from the reinstatement911 PayPal account.

25 116. Investigators reviewed inbox and sent emails from both SUBJECT ACCOUNT
 26 89 and 90 but found no email communication between the two accounts. This is itself
 27

28 ²⁵ [REDACTED] further stated that she felt that she was treated unfairly while employed at Amazon and left her employment after being accepted into an academic program.

evidence that should be seized as it indicates both [REDACTED] (SUBJECT ACCOUNT 89) and Rosenberg (SUBJECT ACCOUNT 90) deleted all email communication between each other, and investigators should be allowed to collect evidence of such omissions and deletions. In addition, information pertinent to the investigation could be found elsewhere in the search warrant return data. For example, the accounts contained other emails, and metadata can be found elsewhere in the account information, including in Google backup drives, which also could contain attachments or data no longer found in email folders.

BACKGROUND REGARDING EMAIL SERVICE PROVIDERS

117. In my training and experience, I have learned that Zoho, Google, 1&1 Mail, and Microsoft provide a variety of on-line services, including electronic mail (“email”) access, to the general public. All four Providers permit users to select custom domain names (e.g., email@custom.com) or to choose generic domain names assigned by the relevant Provider (e.g., email@gmail.com). In the case of Google, the generic domain names are “@gmail.com” and “@googlemail.com.” In the case of Microsoft, one of the generic domain names is “@hotmail.com,” which Microsoft offers through the “Hotmail” service that it previously acquired. Public source records establish that accounts like the SUBJECT ACCOUNTS receive email service from the relevant Providers set out above.

118. Subscribers obtain an account by registering with the relevant Provider. When doing so, the email providers ask the subscriber to provide certain personal identifying information. This information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users, and to help establish who has dominion and control over the account.

119. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on

1 | which the account was created, the length of service, records of log-in (i.e., session) times
2 | and durations, the types of service utilized, the status of the account (including whether the
3 | account is inactive or closed), the methods used to connect to the account, and other log files
4 | that reflect usage of the account. In addition, email providers often have records of the
5 | Internet Protocol address (“IP address”) used to register the account and the IP addresses
6 | associated with particular logins to the account. As with subscriber records, IP address
7 | information can help to identify which computers or other devices were used to access the
8 | email account, which in turn can be used to identify the account’s user or users, and to help
9 | establish who has dominion and control over the account.

10 | 120. In some cases, email account users will communicate directly with an email
11 | service provider about issues relating to the account, such as technical problems, billing
12 | inquiries, or complaints from other users. Email providers typically retain records about
13 | such communications, including records of contacts between the user and the provider's
14 | support services, as well as records of any actions taken by the provider or user as a result of
15 | the communications. In my training and experience, such information may constitute
16 | evidence of the crimes under investigation, because the information can be used to identify
17 | the account’s user or users.

18 | 121. In general, an email that is sent to a subscriber is stored in the subscriber’s
19 | “mail box” on the email provider’s servers until the subscriber deletes the email. When the
20 | subscriber sends an email, it is initiated at the user’s computer, transferred via the Internet to
21 | the provider’s servers, and then transmitted to its end destination. The email provider often
22 | maintains a copy of received and sent emails. Unless the sender specifically deletes an email
23 | from the email provider’s server, the email can remain on the system indefinitely. Even if
24 | the subscriber deletes the email, it may continue to be available on the email provider’s
25 | servers for some period of time.

26 | 122. A sent or received email typically includes the content of the message, source
27 | and destination addresses, the date and time at which the email was sent, and the size and
28 |

1 length of the email. If an email user writes a draft message but does not send it, that message
2 may also be saved by the email provider but may not include all of these categories of data.

3 123. In addition to email, the Providers offer subscribers numerous other services
4 including online chat functionality, cloud-storage services, and location-based services, and
5 web-searching history. Based upon my training and experience, and my review of records in
6 this case, all of the types of information may be evidence of the crimes under investigation in
7 this case.

8 124. There is probable cause to believe that evidence of the crimes listed above is
9 contained in the SUBJECT ACCOUNTS. As explained above, the individuals involved in
10 the conduct under investigation used email, chats, social media, and other online tools to
11 communicate about their bribery and fraud schemes and to execute those schemes. They sent
12 each other information about payments, accounts, schemes, and confidential Amazon
13 information, and they also sent each other copies of that information via electronic
14 communications. Moreover, given the nature of the communications by the defendants and
15 targets of the investigation, which communications refer to other individuals or services that
16 would involve others, there is probable cause to believe the accounts contain
17 communications with Amazon employees and/or others involved in the crimes under
18 investigation. The SUBJECT ACCOUNTS also provide services and functions that can
19 capture and retain records of the evidence, instrumentalities, contraband, and fruits of these
20 crimes. The content of communications is only one example of such evidence,
21 instrumentalities, contraband, and fruits, as other data from the accounts, including data
22 stored in the accounts, the accounts' browsing history, and web-searching history, contacts,
23 IP addresses, registration information, and other services can identify the users of the
24 accounts, serve as evidence of their state of mind with regard to the crimes under
25 investigation, and include misappropriated data from Amazon's network. In addition,
26 information about logging on and logging off accounts can identify who used an account and
27 participated in the crimes under investigation, and information about who sent and received
28 communications can reveal additional members of the schemes under investigation.

125. There is also probable cause to believe that the locations of the users of the SUBJECT ACCOUNTS will serve as evidence of the crimes under investigation. Evidence about the users' location can tie the accounts to particular individuals, and can further be used to establish connections between members of the conspiracy (e.g., in situations where two users are in the same place and their locations can establish the existence of a meeting between them).

126. The Providers are also able to provide information that will assist law enforcement in identifying other accounts associated with the SUBJECT ACCOUNTS, namely, information identifying and relating to other accounts used by the same subscribers. This information includes any forwarding or fetching accounts²⁶ relating to these accounts, all other accounts linked to that account because they were accessed from the same computer (referred to as "cookie overlap"), all other accounts that list the same SMS phone number as that account, all other accounts that list the same recovery email addresses²⁷ as that account, and all other accounts that share the same creation IP address as these accounts. Information associated with these associated accounts will assist law enforcement in determining who controls these accounts and will also help to identify other email accounts and individuals relevant to the investigation.

BACKGROUND REGARDING FACEBOOK²⁸

127. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written

²⁶ A forwarding or fetching account related to the accounts would be a separate email account that can be setup by the user to receive copies of all of the email sent to the account.

²⁷ The recovery email address is an additional email address supplied by the user that is used by the email provider to confirm a username after an email account's creation, help the user if the user is having trouble signing into their account, or alert the user to any unusual activity involving the user's email address.

²⁸ This subsection describing background information about Facebook was taken from the original warrant issued on August 27, 2020, requesting authorization to search SUBJECT ACCOUNT 51. As such, this subsection describes the information likely to be available from the data Facebook provided in response to that original warrant.

1 news, photographs, videos, and other information with other Facebook users, and sometimes
2 with the general public.

3 128. Facebook asks users to provide basic contact and personal identifying
4 information to Facebook, either during the registration process or thereafter. This
5 information may include the user's full name, birth date, gender, contact e-mail addresses,
6 Facebook passwords, Facebook security questions and answers (for password retrieval),
7 physical address (including city, state, and zip code), telephone numbers, screen names,
8 websites, and other personal identifiers. Facebook also assigns a user identification number
9 to each account.

10 129. Facebook users may join one or more groups or networks to connect and
11 interact with other users who are members of the same group or network. Facebook assigns
12 a group identification number to each group. A Facebook user can also connect directly with
13 individual Facebook users by sending each user a "Friend Request." If the recipient of a
14 "Friend Request" accepts the request, then the two users will become "Friends" for purposes
15 of Facebook and can exchange communications or view information about each other. Each
16 Facebook user's account includes a list of that user's "Friends" and a "News Feed," which
17 highlights information about the user's "Friends," such as profile changes, upcoming events,
18 and birthdays.

19 130. Facebook users can select different levels of privacy for the communications
20 and information associated with their Facebook accounts. By adjusting these privacy
21 settings, a Facebook user can make information available only to himself or herself, to
22 particular Facebook users, or to anyone with access to the Internet, including people who are
23 not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate
24 the application of these privacy settings. Facebook accounts also include other account
25 settings that users can adjust to control, for example, the types of notifications they receive
26 from Facebook.

27 131. Facebook users can create profiles that include photographs, lists of personal
28 interests, and other information. Facebook users can also post "status" updates about their

1 whereabouts and actions, as well as links to videos, photographs, articles, and other items
2 available elsewhere on the Internet. Facebook users can also post information about
3 upcoming “events,” such as social occasions, by listing the event’s time, location, host, and
4 guest list. In addition, Facebook users can “check in” to particular locations or add their
5 geographic locations to their Facebook posts, thereby revealing their geographic locations at
6 particular dates and times. A particular user’s profile page also includes a “Wall,” which is a
7 space where the user and his or her “Friends” can post messages, attachments, and links that
8 will typically be visible to anyone who can view the user’s profile.

9 132. Facebook allows users to upload photos and videos, which may include any
10 metadata such as location that the user transmitted when s/he uploaded the photo or video. It
11 also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video.
12 When a user is tagged in a photo or video, he or she receives a notification of the tag and a
13 link to see the photo or video. For Facebook’s purposes, the photos and videos associated
14 with a user’s account will include all photos and videos uploaded by that user that have not
15 been deleted, as well as all photos and videos uploaded by any user that have that user tagged
16 in them.

17 133. Facebook users can exchange private messages on Facebook with other users.
18 These messages, which are similar to e-mail messages, are sent to the recipient’s “Inbox” on
19 Facebook, which also stores copies of messages sent by the recipient, as well as other
20 information. Facebook users can also post comments on the Facebook profiles of other users
21 or on their own profiles; such comments are typically associated with a specific posting or
22 item on the profile. In addition, Facebook has a Chat feature that allows users to send and
23 receive instant messages through Facebook. These chat communications are stored in the
24 chat history for the account. Facebook also has a Video Calling feature, and although
25 Facebook does not record the calls themselves, it does keep records of the date of each call.

26 134. If a Facebook user does not want to interact with another user on Facebook, the
27 first user can “block” the second user from seeing his or her account.
28

1 135. Facebook has a “like” feature that allows users to give positive feedback or
2 connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as
3 webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also
4 become “fans” of particular Facebook pages.

5 136. Facebook has a search function that enables its users to search Facebook for
6 keywords, usernames, or pages, among other things.

7 137. Each Facebook account has an activity log, which is a list of the user’s posts
8 and other Facebook activities from the inception of the account to the present. The activity
9 log includes stories and photos that the user has been tagged in, as well as connections made
10 through the account, such as “liking” a Facebook page or adding someone as a friend. The
11 activity log is visible to the user but cannot be viewed by people who visit the user’s
12 Facebook page.

13 138. Facebook Notes is a blogging feature available to Facebook users, and it
14 enables users to write and post notes or personal web logs (“blogs”), or to import their blogs
15 from other services, such as Xanga, LiveJournal, and Blogger.

16 139. Facebook also has a Marketplace feature, which allows users to post free
17 classified ads. Users can post items for sale, housing, jobs, and other items on the
18 Marketplace.

19 140. In addition to the applications described above, Facebook also provides its
20 users with access to thousands of other applications (“apps”) on the Facebook platform.
21 When a Facebook user accesses or uses one of these applications, an update about that the
22 user’s access or use of that application may appear on the user’s profile page.

23 141. Facebook uses the term “Neoprint” to describe an expanded view of a given
24 user profile. The “Neoprint” for a given user can include the following information from the
25 user’s profile: profile contact information; News Feed information; status updates; links to
26 videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including
27 the friends’ Facebook user identification numbers; groups and networks of which the user is
28 a member, including the groups’ Facebook group identification numbers; future and past

1 event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information
2 about the user’s access and use of Facebook applications.

3 142. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP
4 address. These logs may contain information about the actions taken by the user ID or IP
5 address on Facebook, including information about the type of action, the date and time of the
6 action, and the user ID and IP address associated with the action. For example, if a user
7 views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the
8 profile, and would show when and from what IP address the user did so.

9 143. Social networking providers like Facebook typically retain additional
10 information about their users’ accounts, such as information about the length of service
11 (including start date), the types of service utilized, and the means and source of any
12 payments associated with the service (including any credit card or bank account number). In
13 some cases, Facebook users may communicate directly with Facebook about issues relating
14 to their accounts, such as technical problems, billing inquiries, or complaints from other
15 users. Social networking providers like Facebook typically retain records about such
16 communications, including records of contacts between the user and the provider’s support
17 services, as well as records of any actions taken by the provider or user as a result of the
18 communications.

19 144. As explained herein, information stored in connection with a Facebook account
20 may provide crucial evidence of the “who, what, why, when, where, and how” of the
21 criminal conduct under investigation, thus enabling the United States to establish and prove
22 each element or alternatively, to exclude the innocent from further suspicion. In my training
23 and experience, a Facebook user’s “Neoprint,” IP log, stored electronic communications, and
24 other data retained by Facebook, can indicate who has used or controlled the Facebook
25 account. This “user attribution” evidence is analogous to the search for “indicia of
26 occupancy” while executing a search warrant at a residence. For example, profile contact
27 information, private messaging logs, status updates, and tagged photos (and the data
28 associated with the foregoing, such as date and time) may be evidence of who used or

1 controlled the Facebook account at a relevant time. Further, Facebook account activity can
2 show how and when the account was accessed or used. For example, as described herein,
3 Facebook logs the Internet Protocol (IP) addresses from which users access their accounts
4 along with the time and date. By determining the physical location associated with the
5 logged IP addresses, investigators can understand the chronological and geographic context
6 of the account access and use relating to the crime under investigation. Such information
7 allows investigators to understand the geographic and chronological context of Facebook
8 access, use, and events relating to the crime under investigation. Additionally, Facebook
9 builds geo-location into some of its services. Geo-location allows, for example, users to
10 “tag” their location in posts and Facebook “friends” to locate each other. This geographic
11 and timeline information may tend to either inculcate or exculpate the Facebook account
12 owner.

13 145. Facebook account activity may also provide relevant insight into the Facebook
14 account owner’s state of mind as it relates to the offense under investigation. For example,
15 information on the Facebook account may indicate the owner’s motive and intent to commit
16 a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt
17 (e.g., deleting account information in an effort to conceal evidence from law enforcement).

18 146. Therefore, Facebook records are likely to contain the material described above,
19 including stored electronic communications and information concerning subscribers and
20 their use of Facebook, such as account access information, transaction information, and other
21 account information.

22 //

23 //

24 //

25 //

26 //

27 //

BACKGROUND REGARDING APPLE ID AND iCloud²⁹

147. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

148. Apple has provided a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services have included email, instant messaging, and file storage (including at or around the time when the crimes under investigation were ongoing):

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing

²⁹ The information in this section is based on information published by Apple on its website and reviewed around the time that the crimes under investigation were occurring. The information in this subsection describing background information about Apple and iCloud is largely taken from an earlier affidavit in this case filed in July 2019, closer in time to when the crimes under investigation were on-going and to the issuance in May 2020 of the first warrant for SUBJECT ACCOUNT 43. I have not confirmed that each of these services was available in May 2020, but based on my training and experience and the evidence from this case, I believe this subsection describes many of the services available to iCloud users that were included in the materials provided by Apple in response to the warrant issued in May 2020 and that are sought to be searched in response to this warrant application.

1 allows the user to share those images and videos with other Apple subscribers. iCloud Drive
2 can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and
3 bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the
4 Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity
5 apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and
6 share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep
7 website username and passwords, credit card information, and Wi-Fi network information
8 synchronized across multiple Apple devices.

9 e. Game Center, Apple's social gaming network, allows users of Apple
10 devices to play and share games with each other.

11 f. Find My iPhone allows owners of Apple devices to remotely identify
12 and track the location of, display a message on, and wipe the contents of those devices. Find
13 My Friends allows owners of Apple devices to share locations.

14 g. Location Services allows apps and websites to use information from
15 cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a
16 user's approximate location.

17 h. App Store and iTunes Store are used to purchase and download digital
18 content. iOS apps can be purchased and downloaded through App Store on iOS devices, or
19 through iTunes Store on desktop and laptop computers running either Microsoft Windows or
20 Mac OS. Additional digital content, including music, movies, and television shows, can be
21 purchased through iTunes Store on iOS devices and on desktop and laptop computers
22 running either Microsoft Windows or Mac OS.

23 149. Apple services are accessed through the use of an "Apple ID," an account
24 created during the setup of an Apple device or through the iTunes or iCloud services. A
25 single Apple ID can be linked to multiple Apple services and devices, serving as a central
26 authentication and syncing mechanism.

27 150. An Apple ID takes the form of the full email address submitted by the user to
28 create the account; it can later be changed. Users can submit an Apple-provided email

1 address (often ending in @icloud.com, @me.com, or @mac.com) or an email address
2 associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple
3 ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime)
4 only after the user accesses and responds to a “verification email” sent by Apple to that
5 “primary” email address. Additional email addresses (“alternate,” “rescue,” and
6 “notification” email addresses) can also be associated with an Apple ID by the user.

7 151. Apple captures information associated with the creation and use of an Apple
8 ID. During the creation of an Apple ID, the user must provide basic personal information
9 including the user’s full name, physical address, and telephone numbers. The user may also
10 provide means of payment for products offered by Apple. The subscriber information and
11 password associated with an Apple ID can be changed by the user through the “My Apple
12 ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which
13 the account was created, the length of service, records of log-in times and durations, the
14 types of service utilized, the status of the account (including whether the account is inactive
15 or closed), the methods used to connect to and utilize the account, the Internet Protocol
16 address (“IP address”) used to register and access the account, and other log files that reflect
17 usage of the account.

18 152. Additional information is captured by Apple in connection with the use of an
19 Apple ID to access certain services. For example, Apple maintains connection logs with IP
20 addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and
21 App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s
22 website. Apple also maintains records reflecting a user’s app purchases from App Store and
23 iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail
24 logs” for activity over an Apple-provided email account. Records relating to the use of the
25 Find My iPhone service, including connection logs and requests to remotely lock or erase a
26 device, are also maintained by Apple.

27 153. Apple also maintains information about the devices associated with an Apple
28 ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s

1 IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is
2 the serial number of the device’s SIM card. Similarly, the telephone number of a user’s
3 iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also
4 may maintain records of other device identifiers, including the Media Access Control
5 address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In
6 addition, information about a user’s computer is captured when iTunes is used on that
7 computer to play content associated with an Apple ID, and information about a user’s web
8 browser may be captured when used to access services through icloud.com and apple.com.
9 Apple also retains records related to communications between users and Apple customer
10 service, including communications regarding a particular Apple device or service, and the
11 repair history for a device.

12 154. Apple provides users with five gigabytes of free electronic space on iCloud,
13 and users can purchase additional storage space. That storage space, located on servers
14 controlled by Apple, may contain data associated with the use of iCloud-connected services,
15 including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream,
16 and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork
17 and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs
18 and iCloud Keychain). iCloud can also be used to store iOS device backups, which can
19 contain a user’s photos and videos, iMessages, Short Message Service (“SMS”) and
20 Multimedia Messaging Service (“MMS”) messages, voicemail messages, call history,
21 contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and
22 other data. Records and data associated with third-party apps may also be stored on iCloud;
23 for example, the iOS app for WhatsApp, an instant messaging service, can be configured to
24 regularly back up a user’s instant messages on iCloud Drive. Some of this data is stored on
25 Apple’s servers in an encrypted form but can nonetheless be decrypted by Apple.

26 155. In my training and experience, evidence of who was using an Apple ID and
27 from where, and evidence related to criminal activity of the kind described above, may be
28 found in the files and records described above. This evidence may establish the “who, what,

1 why, when, where, and how” of the criminal conduct under investigation, thus enabling the
2 United States to establish and prove each element or, alternatively, to exclude the innocent
3 from further suspicion. For instance, evidence that identifies the user of an Apple iCloud
4 account at the time that the phone connected to that account engaged in a WhatsApp chat (or
5 sent an email) can establish a direct connection between the phone’s user and the
6 incriminating chat (or email).

7 156. For example, the stored communications and files connected to an Apple ID
8 may provide direct evidence of the offenses under investigation. Based on my training and
9 experience, instant messages, emails, voicemails, photos, videos, and documents are often
10 created and used in furtherance of criminal activity, including to communicate and facilitate
11 the offenses under investigation. In this case, records produced by the compromised
12 Amazon employees establish that multiple records connected to Apple iCloud accounts serve
13 as evidence of the crimes under investigation, including WhatsApp chats backed up to those
14 iCloud accounts and documents saved to their devices for use in connection with the scheme.

15 157. In addition, the user’s account activity, logs, stored electronic communications,
16 and other data retained by Apple can indicate who has used or controlled the account. This
17 “user attribution” evidence is analogous to the search for “indicia of occupancy” while
18 executing a search warrant at a residence. For example, subscriber information, email and
19 messaging logs, documents, and photos and videos (and the data associated with the
20 foregoing, such as geo-location, date and time) may be evidence of who used or controlled
21 the account at a relevant time. As an example, because every device has unique hardware
22 and software identifiers, and because every device that connects to the Internet must use an
23 IP address, IP address and device identifier information can help to identify which computers
24 or other devices were used to access the account. Such information also allows investigators
25 to understand the geographic and chronological context of access, use, and events relating to
26 the crime under investigation.

27 158. Account activity may also provide relevant insight into the account owner’s
28 state of mind as it relates to the offenses under investigation. For example, information on

1 the account may indicate the owner's motive and intent to commit a crime (e.g., information
2 indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account
3 information in an effort to conceal evidence from law enforcement).

4 159. Other information connected to an Apple ID may lead to the discovery of
5 additional evidence. For example, the identification of apps downloaded from App Store
6 and iTunes Store may reveal services used in furtherance of the crimes under investigation or
7 services used to communicate with co-conspirators. In addition, emails, instant messages,
8 Internet activity, documents, and contact and calendar information can lead to the
9 identification of co-conspirators and instrumentalities of the crimes under investigation,
10 including the identities of third-party sellers who participated in the scheme and the products
11 they sold on Amazon Marketplace.

12 160. Therefore, Apple's servers likely contained stored electronic communications
13 and information concerning subscribers and their use of Apple's services, and that data—
14 which Apple previously produced to the FBI, remains in the FBI's possession, and for which
15 this application seeks authorization to search—likely includes evidence, fruit, and
16 instrumentalities of the crimes under investigation.

17 18 **BACKGROUND REGARDING DIGITAL DEVICES**

19 161. As described above and in Attachment B-2, this application seeks permission
20 to search for records in digital devices, including an iPhone, a hard drive, and a thumb drive.
21 Thus, the warrant applied for would authorize the search and seizure of electronic storage
22 media or, potentially, the copying of electronically stored information, all under Rule
23 41(e)(2)(B).

24 162. Based on my training and experience, I know that each of the SUBJECT
25 DEVICES can store large quantities of data, including communications, documents, images,
26 videos, recordings, and other materials that could constitute evidence, fruit, or
27 instrumentalities of the crimes under investigation. I also know that data on digital devices
28 like the SUBJECT DEVICES or remnants of such data can be recovered months or even

1 years after they have been downloaded onto a storage medium, deleted, or viewed via the
2 Internet. Even when files have been deleted, they can be recovered months or years later
3 using forensic tools. This is so because when a person “deletes” a file on a digital device, the
4 data contained in the file does not actually disappear; rather, that data remains on the storage
5 medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted
6 files, may reside in free space or slack space—that is, in space on the storage medium that is
7 not currently being used by an active file—for long periods of time before they are
8 overwritten. In addition, a computer’s operating system may also keep a record of deleted
9 data in a “swap” or “recovery” file.

10 163. Wholly apart from user-generated files, digital devices contain electronic
11 evidence of how they have been used, what they have been used for, and who has used them.
12 To give a few examples, this forensic evidence can take the form of operating system
13 configurations, artifacts from operating system or application operation, file system data
14 structures, and virtual memory "swap" or paging files. Users typically do not erase or delete
15 this evidence, because special software is typically required for that task. However, it is
16 technically possible to delete this information. Similarly, files that have been viewed via the
17 Internet are sometimes automatically downloaded into a temporary Internet directory or
18 "cache."

19 164. I am also aware that defendants and targets of this investigation used encrypted
20 messaging applications, and that records of such messages can be recovered from digital
21 devices found in the residence.

22 165. Digital devices contain not only evidence of what was on the devices but also
23 how the devices were used, the purpose of their use, who used them, and when. Data on
24 digital devices can provide evidence of a file that was once on the device but has since been
25 deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted
26 from a word processing file). Virtual memory paging systems can leave traces of information
27 on the storage medium that show what tasks and processes were recently active. Web
28 browsers, e-mail programs, and chat programs store configuration information on the storage

1 medium that can reveal information such as online nicknames and passwords. Operating
2 systems can record additional information, such as the attachment of peripherals, the
3 attachment of USB flash storage devices or other external storage media, and the times the
4 device was in use. Digital device file systems can record information about the dates files
5 were created and the sequence in which they were created, although this information can
6 later be falsified.

7 166. As explained herein, information stored within a digital device and other
8 electronic storage media may provide crucial evidence of the “who, what, why, when, where,
9 and how” of the criminal conduct under investigation, thus enabling the United States to
10 establish and prove each element or alternatively, to exclude the innocent from further
11 suspicion. In my training and experience, information stored within a digital device or
12 storage media (e.g., registry information, communications, images and movies, transactional
13 information, records of session times and durations, internet history, and anti-virus, spyware,
14 and malware detection programs) can indicate who has used or controlled the device or
15 storage media. This “user attribution” evidence is analogous to the search for “indicia of
16 occupancy” while executing a search warrant at a residence. The existence or absence of
17 anti-virus, spyware, and malware detection programs may indicate whether the computer
18 was remotely accessed, thus inculcating or exculpating the computer owner. Further, digital
19 device and storage media activity can indicate how and when the device or storage media
20 was accessed or used. For example, as described herein, digital devices typically contain
21 information that log: user account session times and durations, computer activity associated
22 with user accounts, electronic storage media that connected with the computer, and the IP
23 addresses through which the digital device accessed networks and the internet. Such
24 information allows investigators to understand the chronological context of digital device or
25 electronic storage media access, use, and events relating to the crime under investigation.
26 Additionally, some information stored within a digital device or electronic storage media
27 may provide crucial evidence relating to the physical location of other evidence and the
28 suspect. For example, images stored on a digital device may both show a particular location

1 and have geolocation information incorporated into its file data. Such file data typically also
2 contains information indicating when the file or image was created. The existence of such
3 image files, along with external device connection logs, may also indicate the presence of
4 additional electronic storage media (e.g., a digital camera or cellular phone with an
5 incorporated camera). The geographic and timeline information described herein may either
6 inculcate or exculpate the device user. Last, information stored within a digital device may
7 provide relevant insight into its user's state of mind as it relates to the offense under
8 investigation. For example, information within the digital device may indicate the owner's
9 motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or
10 consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the
11 computer or password protecting/encrypting such evidence in an effort to conceal it from law
12 enforcement).

13 167. A person with appropriate familiarity with how a digital device works can,
14 after examining this forensic evidence in its proper context, draw conclusions about how it
15 was used, the purpose of its use, who used them, and when. The process of identifying the
16 exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage
17 medium that are necessary to draw an accurate conclusion is a dynamic process. While it is
18 possible to specify in advance the records to be sought, digital device evidence is not always
19 data that can be merely reviewed by a review team and passed along to investigators.
20 Whether data stored on a digital device is evidence may depend on other information stored
21 on the device and the application of knowledge about how it behaves. Therefore, contextual
22 information necessary to understand other evidence also falls within the scope of the warrant.

23 168. Further, in finding evidence of how a digital device was used, the purpose of
24 its use, who used it, and when, sometimes it is necessary to establish that a particular thing is
25 not present on the device. For example, the presence or absence of counter-forensic
26 programs or anti-virus programs (and associated data) may be relevant to establishing the
27 user's intent.
28

1 169. I know that when an individual uses a digital device to create files used in
2 furtherance of a scheme to defraud, the individual's device will generally serve both as an
3 instrumentality for committing the crime, and also as a storage medium for evidence of the
4 crime. The digital device is an instrumentality of the crime because it is used as a means of
5 committing the criminal offense. The digital device is also likely to be a storage medium for
6 evidence of crime. From my training and experience, I believe that a digital device used to
7 commit a crime of this type may contain: data that is evidence of how the device was used;
8 data that was sent or received; notes as to how the criminal conduct was achieved; records of
9 Internet discussions about the crime; and other records that indicate the nature of the offense.

10 11 CONCLUSION

12 170. Based on the foregoing, I believe there is probable cause to believe that
13 evidence, instrumentalities, contraband, and/or fruits of violations of Title 18, United States
14 Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1030 (Unauthorized Access
15 to a Protected Computer), 1343 (Wire Fraud), 1349 (Conspiracy to Commit Wire Fraud), and
16 1952 (Travel Act) will be found in the SUBJECT ACCOUNTS and SUBJECT DEVICES,
17 as more fully described in Attachments A-1 and A-2 to this Affidavit. I therefore request
18 that the Court issue warrants authorizing a search of the SUBJECT ACCOUNTS and
19 SUBJECT DEVICES, for the items more fully described in Attachments B-1 and B-2 hereto,
20 incorporated herein by reference, and the seizure of any such items found therein.

21 //

22 //

23 //

24 //

25 //

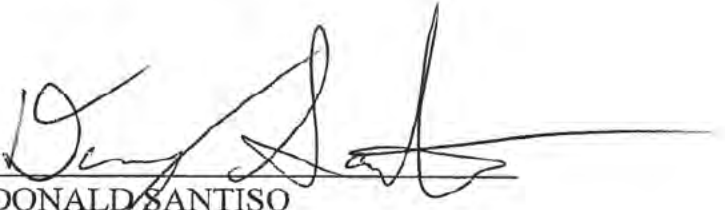
26 //

27 //

28 //

1 171. Based on the foregoing, I request that the Court issue the proposed search
2 warrants. Because the materials to be searched are within the possession of the FBI,
3 reasonable cause exists to permit the execution of the requested warrant at any time in the
4 day or night.

5 172. The affidavit and application are being presented by reliable electronic means
6 pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).
7
8
9

10 
11 DONALD SANTISO
12 Special Agent
13 Federal Bureau of Investigation

14 The above-named agent provided a sworn statement attesting to the truth of the
15 contents of the foregoing affidavit by telephone on the 5th day of October, 2022.
16
17

18 
19 HON. BRIAN A. TSUCHIDA
20 Chief United States Magistrate Judge
21
22
23
24
25
26
27
28

ATTACHMENT A-1

Subject Accounts to be Searched

The electronically stored data, information, and communications provided by service providers in response to earlier search warrants issued in this investigation and currently stored in evidence at the FBI's Office in Seattle, Washington, as further described below:

a. All data, information, communications, and logs related to the account [REDACTED] ("SUBJECT ACCOUNT 80"), which were stored at premises controlled by Zoho Corporation ("Zoho") headquartered in Pleasanton, California; produced to investigators by Zoho; and are currently stored at the FBI Office in Seattle, Washington;³⁰

b. All data, information, communications, and logs related to the accounts [REDACTED] ("SUBJECT ACCOUNT 81"), [REDACTED] ("SUBJECT ACCOUNT 82"), [REDACTED] ("SUBJECT ACCOUNT 84"), [REDACTED] ("SUBJECT ACCOUNT 85"), [REDACTED] ("SUBJECT ACCOUNT 86"), [REDACTED] ("SUBJECT ACCOUNT 87"), [REDACTED] ("SUBJECT ACCOUNT 88"), and [REDACTED] ("SUBJECT ACCOUNT 89") which were stored at premises controlled by Google LLC ("Google") headquartered in Mountain View, California; produced to investigators by Google; and are currently stored at the FBI Office in Seattle, Washington;

c. All data, information, communications, and logs related to the account [REDACTED] ("SUBJECT ACCOUNT 83"), which were stored at premises controlled by Microsoft Corporation ("Microsoft") headquartered in Redmond, Washington; produced to investigators by Microsoft; and are currently stored at the FBI Office in Seattle, Washington;

³⁰ Brackets have been placed around the @ symbols in the email addresses discussed herein, to ensure that those email addresses are not inadvertently hyperlinked in any electronic version of this document.

1 d. All data, information, communications, and logs related to the
2 Apple iCloud account registered to nishadkunj[[@](#)]icloud.com (“SUBJECT
3 ACCOUNT 43”), which were stored at premises controlled by Apple, Inc. (“Apple”)
4 headquartered at One Apple Park Way, Cupertino, California; produced to
5 investigators by Apple; and are currently stored at the FBI Office in Seattle,
6 Washington;

7 e. All data, information, communications, and logs related to the
8 Facebook account bearing digital sign identifier [REDACTED] (“SUBJECT
9 ACCOUNT 51”), which were stored at premises controlled by Meta Platforms, Inc.
10 (“Meta”) headquartered at 1601 Willow Road, Menlo Park, California; produced to
11 investigators by Meta; and are currently stored at the FBI Office in Seattle,
12 Washington; and

13 f. All data, information, communications, and logs related to the
14 account amzLamarnt[[@](#)]mail.com (“SUBJECT ACCOUNT 90”), which were stored
15 at premises controlled by 1&1 Mail & Media, Inc. (“1&1 Mail”) located at 701 Lee
16 Road, Suite 300, Chesterbrook, Pennsylvania; produced to investigators by 1&1 Mail;
17 and are currently stored at the FBI Office in Seattle, Washington.

18
19 (Brackets have been placed around the @ symbols in the email addresses listed above,
20 to ensure that those email addresses are not inadvertently hyperlinked in any electronic
21 version of this document.)
22
23
24
25
26
27
28

ATTACHMENT A-2

Subject Devices to be Searched

The digital devices provided to United States authorities by India's Central Bureau of Investigation in response to a request for assistance pursuant to a Mutual Legal Assistance Treaty that were seized from [REDACTED], India, on or around February 21, 2021, and that are currently stored at the FBI's Office in Seattle, Washington, and that meet the following descriptions:

- a. FBI Evidence item 1B110 - 128 GB SanDisk Thumb Drive,
- b. FBI Evidence item – 1B111 - 1 TB WD Hard Drive, and
- c. FBI Evidence item 1B112 - Black iPhone 8 Plus.

ATTACHMENT B-1**Information to be seized by the government**

All information described in Attachment A-1 that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1028A (Aggravated Identity Theft), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected Computer), 1343 (Wire Fraud), 1349 (Conspiracy to Commit Wire Fraud), and 1952 (Travel Act), those violations occurring from on or about January 1, 2017, through January 19, 2021, for the accounts and data listed in Attachment A-1 (collectively the “Accounts”), including the following:

- a. Records that serve to identify any person who uses or accesses the Accounts, or who exercises in any way any dominion or control over the Accounts;
- b. Records that relate to planned, attempted, or successful conduct with respect to seller accounts operating on the Amazon Marketplace online platform, or products sold on that platform;
- c. Records that relate to information maintained by Amazon in connection with the operation of the Amazon Marketplace, including information regarding the operation of the Amazon Marketplace, information regarding the participants in the Amazon Marketplace, information regarding products sold on the Amazon Marketplace, information regarding metrics of Amazon Marketplace activity, information relating to enforcement actions (e.g., suspensions and reinstatements) taken with respect to sellers on Amazon Marketplace, and information relating to communications between third parties and Amazon with respect to activity on the Amazon Marketplace;
- d. Records that relate to access to computer systems operated or controlled by Amazon;
- e. Records that relate to tools, programs, approvals, permissions, processes, and mechanisms used by Amazon to operate and regulate its computer

1 systems and the Amazon Marketplace;

2 f. Records that relate to persons (both fictitious and actual) and
3 products involved in e-commerce;

4 g. Records that relate to the use of aliases and attempts to hide or
5 conceal a person's identity;

6 h. Records relating to planned, attempted, or successful transfers of
7 funds in connection with the crimes specified above;

8 i. Records relating to the recruitment of employees of Amazon (or
9 Amazon-affiliated entities) to take actions in exchange for things of value, including
10 commercial bribes;

11 j. Records relating to the planning for, attempted, or successful
12 payment of bribes to Amazon employees;

13 k. Records related to the planning for, attempted, or successful
14 transmission of false statements or omissions to Amazon (or Amazon-affiliated
15 entities);

16 l. Records that constitute communications in furtherance of the
17 crimes set out above;

18 m. Records that indicate the state of mind of any person, including
19 the user of the Accounts, with regard to the crimes set out above;

20 n. Records that indicate efforts to destroy or delete evidence of the
21 crimes set out above;

22 o. Records that may identify assets including bank accounts,
23 commodities accounts, trading accounts, personal property and/or real estate that may
24 represent proceeds of fraud or are traceable to such proceeds;

25 p. Records that may reveal the current or past location of the
26 individual or individuals using the Accounts or involved in the crimes set out above;

27 q. Records that indicate the user of digital devices, including
28 cellular telephones, computers, servers, hard drives, and other digital storage

1 mediums;

2 r. Records that may reveal the identities of and relationships
3 between co-conspirators;

4 s. Records that may identify any alias names, online user names,
5 “handles” and/or “nics” of those who exercise in any way any dominion or control
6 over the Accounts, as well as records or information that may reveal the true identities
7 of these individuals;

8 t. Other log records, including IP address captures, associated with
9 the Accounts;

10 u. Subscriber records associated with the Accounts, including 1)
11 names, email addresses, and screen names; 2) physical addresses; 3) records of
12 session times and durations; 4) length of service (including start date) and types of
13 services utilized; 5) telephone or instrument number or other subscriber number or
14 identity, including any temporarily assigned network address such as internet protocol
15 address, media access card addresses, or any other unique device identifiers recorded
16 by the service providers for the Accounts in relation to an account; 6) account log
17 files (login IP address, account activation IP addresses, and IP address history); 7)
18 detailed billing records/logs; 8) means and source of payment; and 9) lists of all
19 related accounts;

20 v. Records of communications between the service providers for the
21 Accounts (specifically, Zoho, Google, Microsoft, Apple, Meta, and 1&1) and any
22 person purporting to be the account holder about issues relating to the account, such
23 as technical problems, billing inquiries, or complaints from other users about the
24 specified account. This is to include records of contacts between the subscriber and
25 the provider’s support services, as well as records of any actions taken by the provider
26 or subscriber as a result of the communications;

27 w. Device identification numbers, MEID, and cellular telephone
28 numbers for any devices that accessed the Account.

1 The requested warrant authorizes a review of electronic storage media, electronically
2 stored information, communications, and other records and information seized, copied or
3 disclosed pursuant to the warrant in order to locate evidence, fruits, and instrumentalities
4 described in this warrant. The review of this electronic data may be conducted by any
5 government personnel assisting in the investigation, who may include, in addition to law
6 enforcement officers and agents, attorneys for the government, attorney support staff, and
7 technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the
8 seized, copied, or disclosed electronic data to the custody and control of attorneys for the
9 government and their support staff for their independent review.

10 The term “records” used in Attachment B-1 includes data and information found in
11 any form that meets the substantive categories set forth above.

12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT B-2

Information to be seized by the government

All information described in Attachment A-2 that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1028A (Aggravated Identity Theft), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected Computer), 1343 (Wire Fraud), 1349 (Conspiracy to Commit Wire Fraud), and 1952 (Travel Act), those violations occurring from on or about January 1, 2017, through September 16, 2020, for the digital devices (and data contained on those devices) listed in Attachment A-2 (collectively the “Devices”), including the following:

- a. Records that serve to identify any person who uses or accesses the Devices, or who exercises in any way any dominion or control over the Devices;
- b. Records that relate to planned, attempted, or successful conduct with respect to seller accounts operating on the Amazon Marketplace online platform, or products sold on that platform;
- c. Records that relate to information maintained by Amazon in connection with the operation of the Amazon Marketplace, including information regarding the operation of the Amazon Marketplace, information regarding the participants in the Amazon Marketplace, information regarding products sold on the Amazon Marketplace, information regarding metrics of Amazon Marketplace activity, information relating to enforcement actions (e.g., suspensions and reinstatements) taken with respect to sellers on Amazon Marketplace, and information relating to communications between third parties and Amazon with respect to activity on the Amazon Marketplace;
- d. Records that relate to access to computer systems operated or controlled by Amazon;
- e. Records that relate to tools, programs, approvals, permissions, processes, and mechanisms used by Amazon to operate and regulate its computer

1 systems and the Amazon Marketplace;

2 f. Records that relate to persons (both fictitious and actual) and
3 products involved in e-commerce;

4 g. Records that relate to the use of aliases and attempts to hide or
5 conceal a person's identity;

6 h. Records relating to planned, attempted, or successful transfers of
7 funds in connection with the crimes specified above;

8 i. Records relating to the recruitment of employees of Amazon (or
9 Amazon-affiliated entities) to take actions in exchange for things of value, including
10 commercial bribes;

11 j. Records relating to the planning for, attempted, or successful
12 payment of bribes to Amazon employees;

13 k. Records related to the planning for, attempted, or successful
14 transmission of false statements or omissions to Amazon (or Amazon-affiliated
15 entities);

16 l. Records that constitute communications in furtherance of the
17 crimes set out above;

18 m. Records that indicate the state of mind of any person, including
19 the user of the Devices, with regard to the crimes set out above;

20 n. Records that indicate efforts to destroy or delete evidence of the
21 crimes set out above;

22 o. Records that may identify assets including bank accounts,
23 commodities accounts, trading accounts, personal property and/or real estate that may
24 represent proceeds of fraud or are traceable to such proceeds;

25 p. Records that may reveal the current or past location of the
26 individual or individuals using the Devices or involved in the crimes set out above;

27 q. Records that indicate the user of digital devices, including
28 cellular telephones, computers, servers, hard drives, and other digital storage

1 mediums;

2 r. Records that may reveal the identities of and relationships
3 between co-conspirators;

4 s. Records that may identify any alias names, online user names,
5 “handles” and/or “nics” of those who exercise in any way any dominion or control
6 over the Devices or any accounts, as well as records or information that may reveal
7 the true identities of these individuals;

8 t. Other log records, including IP address captures, associated with
9 the Devices;

10 u. Subscriber records associated with any online accounts accessed
11 from the Devices and related to the crimes set forth above, including 1) names, email
12 addresses, and screen names; 2) physical addresses; 3) records of session times and
13 durations; 4) length of service (including start date) and types of services utilized;
14 5) telephone or instrument number or other subscriber number or identity, including
15 any temporarily assigned network address such as internet protocol address, media
16 access card addresses, or any other unique device identifiers recorded by service
17 providers in relation to the account; 6) account log files (login IP address, account
18 activation IP addresses, and IP address history); 7) detailed billing records/logs; 8)
19 means and source of payment; and 9) lists of all related accounts;

20 v. Device identification numbers, MEID, and cellular telephone
21 numbers for any devices that accessed the Account.

22 The requested warrant authorizes a review of electronic storage media, electronically
23 stored information, communications, and other records and information seized, copied or
24 disclosed pursuant to the warrant in order to locate evidence, fruits, and instrumentalities
25 described in this warrant. The review of this electronic data may be conducted by any
26 government personnel assisting in the investigation, who may include, in addition to law
27 enforcement officers and agents, attorneys for the government, attorney support staff, and
28 technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the

1 seized, copied, or disclosed electronic data to the custody and control of attorneys for the
2 government and their support staff for their independent review.

3 The term “records” used in Attachment B-2 includes data and information found in
4 any form that meets the substantive categories set forth above.